Vulnerabilities in Baseboard Management Controllers: Risks and Mitigation Strategies in the IIoT Environment

Jackson Júnior[1], Sérgio Ivan[1,2], and Pedro Pinto[1,3]

[1] ADiT-LAB, Instituto Politécnico de Viana do Castelo, IPVC, Portugal
jacksonjunior@ipvc.pt
[2] CiTin, Portugal
sil@estg.ipvc.pt
[3] INESC TEC, Portugal
pedropinto@estg.ipvc.pt

Abstract. Vulnerabilities in Baseboard Management Controllers (BMCs) have a high impact on the Industrial Internet of Things (IIoT) environment. Recently, a set of vulnerabilities in BMCs disclosed by Nozomi Networks expose Operational Technology (OT) and IIoT networks to remote attacks.
This paper reviews a set of vulnerabilities in BMC affecting IIoT devices and discusses the risks and implications of the vulnerabilities found, and how they can be mitigated.
The discovery of vulnerabilities in BMC highlights the urgent need for a comprehensive and multifaceted approach to securing the IIoT environment. It is concluded that a general improvement in the security of BMC could be achieved by adopting the open-source philosophy and standardizing the hardware interface.

Keywords: BMC (Baseboard Management Controller) · firmware vulnerabilities · IIoT (Industrial Internet of Things).

1 Introduction

The Industrial Internet of Things (IIoT) has revolutionized the way industrial systems operate, providing endless possibilities for connectivity and automation. However, with this, increased reliance on technology comes a need for robust security measures to protect against potential vulnerabilities and attacks.

Baseboard Management Controllers (BMCs) are specialized service processors traditionally found in server motherboards and used for remote monitoring and managing a host system, including performing low-level system operations such as firmware flashing and power control. However, in recent years, BMCs have also been used increasingly in devices Operational Technology (OT) and IIoT. While BMCs offer convenience through remote monitoring and management, they also present a broader attack surface and can increase the overall risk of a system if not adequately protected.

Recently, security company Nozomi Networks analyzed a BMC from Taiwanese vendor Lanner Electronics and uncovered 13 vulnerabilities that affect their IAC-AST2500A expansion card [1]. The firmware of the IAC-AST2500A [2] is based on the American Megatrends (AMI) MegaRAC SP-X solution [3], which is also used by major brands such as Asus, Dell, Gigabyte, HP, Lenovo, and nVidia [4].

This research aims to review the vulnerabilities discovered by Nozomi Networks in BMCs and to discuss the potential risks and consequences of these vulnerabilities on OT and IIoT networks. Additionally, it aims to provide recommendations for increasing

security and mitigating these vulnerabilities, specifically in devices utilizing the AMI MegaRAC SP-X solution [4].

The rest of the paper is organized as follows. Section 2, presents related work. Section 3 presents the results. Section 4 discusses the findings, implications, and how the vulnerabilities can be mitigated. Section 5 provides the conclusions and outlines the future research directions.

2 Related Works

In the field of Internet of Things (IoT) and IIoT security, several works have addressed the issue of detecting and preventing cyber attacks on connected devices. Karande et al. [5] presents a review of the state of the art of IoT security needs and implementation mechanisms and proposes a real-time security attack detection system using a Google cloud platform. The work demonstrates the experimental setup and performs a performance analysis of the proposed system. Xenofontos et al. [6] present a systematic review of IoT security from three major sectors: consumer, commercial, and industrial. The work provides definitions for each sector and discusses operational requirements, implicit security constraints, mission criticality, and potential outcomes in the event of a compromise targeting the respective IoT sectors.

In the field of BMC security, Latzo et a. [7] introduce a memory acquisition tool called BMCLeech to perform unobtrusive memory forensics on operating systems. The tool is based on a BMC and exploits the Direct Memory Access (DMA) capability of the host through the BMC. BMCLeech is capable of acquiring a system's memory unobtrusively, as it is a standard device on many systems, and the host, therefore, cannot distinguish between "good" activities (such as server administration) and "bad" activities (taking memory snapshots). Furthermore, BMCLeech is capable of transparently acquiring memory for the operating system, making it a viable option for the forensic analysis of operating systems.

Frazelle [8] discuss the various security concerns related to BMCs, including the fact that the stack Intelligent Platform Management Interface (IPMI) was not designed with security in mind and has a history of vulnerabilities. The work also highlights the issue of proprietary software and vulnerabilities in BMC itself, citing examples such as USBAnywhere and Pantsdown vulnerabilities. In addition, the paper discusses the BMC's access to host firmware via Serial Peripheral Interface (SPI) and host memory through DMA, making it a prime target for hackers. The lack of a secure boot in BMC firmwares is also a concern mentioned in the article. In general, the work emphasizes the importance of improving the security of BMCs, given its privileged access and critical role in the operation of the servers.

Frazelle [9] presents a comprehensive overview of the importance of secure booting mechanisms in ensuring hardware and software integrity in modern computing systems. The work discusses the concept of a hardware root of trust, which aims to verify that the software installed in all hardware components is the intended software. It also introduces the Trusted Platform Module (TPM), a standard for a microchip designed to secure hardware through cryptographic keys, and its role in attestation, which reports on the state of the hardware and software configuration to establish code identity to remote or

local verifiers. The paper also discusses the challenges of implementing a hardware root of trust, such as the lack of transparency in proprietary firmware and the need for open-source options. It concludes by stressing the importance of secure booting mechanisms in today's security landscape, given the increasing threat of supply chain attacks, evil maid attacks, and cloud provider vulnerabilities.

Farmer [10] presents an important work in the field of BMC security, which includes a scan of the IPMI protocol across the internet and identifies a high percentage of vulnerable BMCs that could be compromised through basic configuration and protocol weaknesses. The work highlights the security risks of BMCs, including vulnerabilities in the IPMI protocol and poor implementations by BMC manufacturers, and discusses the impact of these vulnerabilities on the security of servers and large-scale data centers that rely heavily on IPMI for management and deployment. The authors also argue that the widespread use of vulnerable BMCs will continue to be a problem for years to come due to the large number of servers that include them.

Despite the critical nature of the issue, the topic of BMCs security is just beginning to be discussed in academia. This study aims to contribute to this body of research by disseminating security vulnerabilities identified by the industry and proposing security recommendations to mitigate similar vulnerabilities in equipped devices IoT and IIoT.

3 Vulnerabilities in Baseboard Management Controllers

Nozomi Networks detected 13 vulnerabilities in Lanner Electronics BMCs. Among these, five are rated as 9 or higher on the Common Vulnerability Scoring System (CVSS), thereby indicating their high severity. These vulnerabilities include CVE-2021-26727, CVE-2021-26728, CVE-2021-26729, CVE-2021-26730, and CVE-2021-26731.

Apart from CVE-2021-26730, each of the vulnerabilities is categorized under Common Weakness Enumeration (CWE), CWE-787, and CWE-77, both of which are associated with code execution. *CWE*-787, also known as Out-of-bounds Write, is a type of vulnerability in which an application unintentionally writes data beyond the established boundary of a memory structure, such as a buffer or array [11]. *CWE*-77, designated as Improper Neutralization of Special Elements Used in a Command ('Command Injection'), describes a system weakness whereby an application or system may inadvertently allow user input to direct the execution of system commands or queries, without conducting adequate input validation or sanitization. They can be exploited through the "spx_restservice" web service, which is accessible through the web interface of the IAC-AST2500A expansion card.

The remaining 8 vulnerabilities found (CVE-2021-26732, CVE-2021-26733, CVE-2021-44776, CVE-2021-44467, CVE-2021-44769, CVE-2021-46279, CVE-2021-45925, CVE-2021-4228) are of medium or low severity.

The vulnerabilities related to CWE -862 (CVE-2021-26732, CVE-2021-26733, CVE-2021-44776) represent weaknesses in authorization, allowing unauthorized access to sensitive data or actions. Their exploitation can lead to altered network configurations, host disruption, and Cross-Site Scripting (XSS) attacks.

Further vulnerabilities include the capability for active session termination (CVE-2021-44467), Denial-of-Service (DoS) condition on BMC (CVE-2021-44769), session

hijacking (CVE-2021-46279), legitimate username discovery (CVE-2021-45925), and Man-in-the-Middle (MitM) attacks (CVE-2021-4228).

The criticality of these vulnerabilities and possible mitigation strategies are discussed in the following section.

4 Discussion

It is crucial to note that the potential impact of these vulnerabilities extends beyond financial concerns and encompasses significant risks to human lives, national security, and political stability. Previous incidents have highlighted the severity of these risks, with reported attacks on food manufacturers [12], water treatment facilities [13], and the oil industry [14] resulting in food shortages, the potential poisoning of thousands of people, and potential environmental disasters. The potential for a chain reaction of such incidents further emphasizes the urgency and gravity of addressing these vulnerabilities in industrial control systems and IIoT networks.

Firewall and Intrusion Prevention System (IPS) security solutions typically focus on blocking external threats at the perimeter level of a network, but they are not efficient in controlling or stopping the propagation of threats that have already breached the network [15]. Traditional measures, such as firewalls and IPS, used in isolation, are insufficient to mitigate the vulnerabilities presented in this research. Therefore, a multifaceted approach is necessary to address the vulnerabilities in BMCs that have been discussed in this investigation.

On the one hand, several steps can be taken to mitigate vulnerabilities in IIoT systems in their current context. This includes implementing a comprehensive security policy that focuses on raising awareness about the importance of IIoT devices, implementing a configuration management policy that includes regular firmware checks and updates, implementing multi-factor authentication methods, using password managers and physical cryptographic key tokens to enforce the use of strong passwords, and implementing network segmentation based on device attributes, service types, and network information to prevent the direct exposure of BMCs to the Internet and ensure secure connections with multi-factor authentication [16].

On the other hand, a general improvement in the security of BMCs can also be achieved by adopting the open-source philosophy. Projects such as OpenBMC and U-bmc, which use thread-safe programming languages and replace the vulnerable IPMI protocol with gRPC, provide a promising approach by promoting transparency and community-driven development. Furthermore, initiatives such as RunBMC, which standardizes the hardware interface for BMCs and allows isolation and locking of the subsystem, can also improve security by making it easier to replace or update BMCs and integrate additional security measures. By open-sourcing the software at the lowest levels of the stack, we can provide visibility into the code running with the most privileges on the systems. This approach will lead to more eyes scrutinizing the code, encourage more minimal architectures, and lessen the risk that systems are caught off guard in the future [8].

Evidently, these open-source and hardware standardization initiatives should consider measures such as not using pre-programmed passwords on IIoT devices, meaning

that all passwords must be unique and should not return to their original credentials state upon factory reset [17]. Furthermore, devices should have viable hardware security schemes, such as cryptographic processors, Physically Unclonable Functions (PUFs), Hash-based Message Authentication Codes (HMACs), and random key generators [18, 19]. These alternatives also make it cheaper for manufacturers to ensure long-term updates of this hardware and software.

The vulnerabilities discovered in Lanner Electronic's BMCs pose a significant threat not only to the security of IIoT and OT systems but also to human lives.

The industry must take a multifaceted approach to address these vulnerabilities, focusing on short-term mitigation strategies, such as network segregation and regular firmware updates, and long-term solutions, such as adopting open-source software and hardware development.

5 Conclusion

This research aimed to investigate and provide information on the potential vulnerabilities in BMCs and their impact on the environment IIoT. Specifically, we focused on the recent discovery of vulnerabilities in BMCs made by Nozomi Networks that can expose OT and IIoT networks to remote attacks.

In the discussion section, the implications of the vulnerabilities found and how they can be mitigated are presented. We highlighted that traditional measures such as firewalls and IPS, used in isolation, are insufficient to mitigate the vulnerabilities presented in this research. Consequently, a multifaceted approach is necessary to address the vulnerabilities in BMCs.

Therefore, it was suggested that a general improvement in the security of BMCs could be achieved by adopting the open source philosophy and standardizing the hardware interface, jointly by implementing a comprehensive security policy that focuses on raising awareness of the importance of IIoT devices, managing configuration that includes regular firmware checks and updates, multifactor authentication methods, and network segmentation based on device attributes, service types, and generated information.

It is important to note that this research is based on a specific discovery of vulnerabilities made by Nozomi Networks in a specific brand of BMCs. While the findings provide valuable information, it is crucial to understand that the vulnerabilities and risks discussed may not apply to other brands or models of BMCs. However, the security measures suggested in this research can provide general protection, as the vulnerabilities were classified into the categories of Service, Communication, and Device according to a taxonomy used as a reference.

Future developments of this research could involve investigating ways to make the use of cryptographic and authentication mechanisms on resources-limited IIoT devices viable, such as the use of cryptographic processors, PUFs, HMACs, and random key generators. This could involve exploring new techniques to secure these devices, while also addressing the challenges of implementing these mechanisms on devices with limited resources.

In conclusion, the discovery of vulnerabilities in BMCs by Nozomi Networks highlights the urgent need for a comprehensive and multifaceted approach to securing in-

dustrial control systems and the Internet of Industrial Things. Failure to address these vulnerabilities can have devastating consequences, not only for the financial well-being of organizations but also for human lives.

Acknowledgment

This study was developed in the context of the Master of Cybersecurity Programme at the Polytechnic University of Viana do Castelo, Portugal.

This work was supported by the Norte Portugal Regional Operational Program (NORTE 2020), under the PORTUGAL 2020 Partnership Agreement, through the European Regional Development Fund (ERDF), within the project "Cybers SeC IP" (NORTE-01-0145-FEDER-000044).

References

1. Nozomi Networks Labs. Vulnerabilities in BMC Firmware Affect OT/IoT Device Security – Part 1, nov 2022.
2. Lanner Electronics Inc. IAC-AST2500 — Network Appliance — uCPE SD-WAN— MEC Server — Intelligent Edge Appliance.
3. AMI. Megarac.
4. American Megatrends. System-on-Chip Remote Management Toolset MegaRAC SP-X. (Accessed on 20/12/2022).
5. Jalindar Karande and Sarang Joshi. Real-Time Detection of Cyber Attacks on the IoT Devices. In *Real-Time Detection of Cyber Attacks on the IoT Devices*, 2020.
6. Christos Xenofontos, Graduate Student Member, Ioannis Zografopoulos, Charalambos Konstantinou, Senior Member, Alireza Jolfaei, Muhammad Khurram Khan, and Kim-Kwang Raymond Choo. Consumer, Commercial, and Industrial IoT (In)Security: Attack Taxonomy and Case Studies; Consumer, Commercial, and Industrial IoT (In)Security: Attack Taxonomy and Case Studies. *IEEE Internet of Things Journal*, 9(1), 2022.
7. Tobias Latzo, Julian Brost, and Felix Freiling. BMCLeech: Introducing Stealthy Memory Forensics to BMC. *Forensic Science International: Digital Investigation*, 32, apr 2020.
8. Jessie Frazelle. Opening up the baseboard management controller. *Communications of the ACM*, 63(2):38–40, jan 2020.
9. Jessie Frazelle. Securing the Boot Process. *Queue*, 17(6):5–21, dec 2019.
10. Dan Farmer. Sold Down the River. (Accessed on 20/12/2022), jun 2014.
11. National Institute of Standards and Technology. CWE - CWE-787: Out-of-bounds Write (4.9).
12. Yoni Shohet. Ransomware Attacks Hit Manufacturing - Are You Vulnerable?, mar 2019.
13. Amin Hassanzadeh, Amin Rasekh, Stefano Galelli, Mohsen Aghashahi, Riccardo Taormina, Avi Ostfeld, and Katherine Banks. A Review of Cybersecurity Incidents in the Water Sector. *Journal of Environmental Engineering*, 146(5), jan 2020.
14. Martin Giles. Triton is the world's most murderous malware, and it's spreading, mar 2019.
15. Salim Mahamat Charfadine, Olivier Flauzac, Florent Nolot, Cyril Rabat, and Carlos Gonzalez. Secure exchanges activity in function of event detection with the sdn. In Gervais Mendy, Samuel Ouya, Ibra Dioum, and Ousmane Thiaré, editors, *e-Infrastructure and e-Services for Developing Countries*, pages 315–324, Cham, 2019. Springer International Publishing.
16. Jaedeok Lim, Seongyoung Sohn, and Jeongnyeo Kim. Proposal of smart segmentation framework for preventing threats from spreading in iot. In *2020 International Conference on Information and Communication Technology Convergence (ICTC)*, pages 1745–1747, 2020. (Accessed on 23/12/2022).
17. Jane Wakefield. Huge fines and a ban on default passwords in new UK law, nov 2021.
18. Charalambos Konstantinou. Derauth: A battery-based authentication scheme for distributed energy resources. In *Proceedings of IEEE Computer Society Annual Symposium on VLSI, ISVLSI*, pages 560–567. IEEE Computer Societyhelp@computer.org, July 2020. Generated from Scopus record by KAUST IRTS on 2022-09-13.

19. Ioannis Zografopoulos, Juan Ospina, and Charalambos Konstantinou. Special session: Harness the power of ders for secure communications in electric energy systems. In *2020 IEEE 38th International Conference on Computer Design (ICCD)*, pages 49–52, 2020.