Harden Baseboard Management Controllers

Summary

Baseboard management controllers (BMCs) are trusted components designed into a computer's hardware that operate separately from the operating system and firmware to allow for remote management and control, even when the system is shut down. This Cybersecurity Information Sheet (CSI), authored by the National Security Agency (NSA) and the Cybersecurity and Infrastructure Security Agency (CISA), highlights threats to BMCs and details actions organizations can use to harden them. NSA and CISA encourage all organizations managing relevant servers to apply the recommended actions in this CSI.

Malicious actors target overlooked firmware

A BMC differs from the basic input output system (BIOS) and the Unified Extensible Firmware Interface (UEFI), which have a later role in booting a computer, and management engine (ME), which has different remote management functionality. BMC firmware is highly privileged, executes outside the scope of operating system (OS) controls, and has access to all resources of the server-class platform on which it resides. It executes the moment power is applied to the server. Therefore, boot to a hypervisor or OS is not necessary as the BMC functions even if the server is shutdown.

Most BMCs provide network-accessible configuration and management, and BMC management solutions administer large numbers of servers without requiring a physical touch. They take the form of a dedicated circuit chip with discrete firmware that must be maintained separately from automated or OS-hosted patching solutions. Most BMCs do not provide integration with user account management solutions. Administrators must perform updates and all administrative actions affecting BMCs via commands delivered over network connections.

Many organizations fail to take the minimum action to secure and maintain BMCs. Hardened credentials, firmware updates, and network segmentation options are frequently overlooked, leading to a vulnerable BMC. A vulnerable BMC broadens the attack vector by providing malicious actors the opportunity to employ tactics such as establishing a beachhead with pre-boot execution potential. [1] Additionally, a malicious actor could disable security solutions such as the trusted platform module (TPM) or UEFI secure boot, manipulate data on any attached storage media, or propagate implants or disruptive instructions across a network infrastructure. Traditional tools and security features including endpoint detection and response (EDR) software, intrusion detection/prevention systems (IDS/IPS), anti-malware suites, kernel security

enhancements, virtualization capabilities, and TPM attestation are ineffective at mitigating a compromised BMC. For these reasons, NSA and CISA recommend organizations pay attention to the security of their BMCs and apply the hardening actions detailed in the following section.

Recommended actions

These recommended actions align with the cross-sector cybersecurity performance goals (CPGs) CISA and the National Institute of Standards and Technology (NIST) developed. The CPGs provide a minimum set of practices and protections that CISA and NIST recommend all organizations implement. Visit CISA's Cross-Sector Cybersecurity Performance Goals for more information on the CPGs, including additional recommended baseline protections.

1. Protect BMC credentials

Change the default BMC credentials as soon as possible. Establish unique user accounts for administrators, if supported. Always use strong passwords compliant with NIST guidelines such as SP 800-63B. [2] Do not expose default credentials to an internet connection or untrusted segment of an enclave [CPG 2.A, 2.B, 2.C, 2.E, 2.L].

2. Enforce VLAN separation

Establish a virtual local area network (VLAN) to isolate BMC network connections since many BMC products have a dedicated network port not shared with the OS or virtual machine manager (VMM). Limit the endpoints that may communicate with BMCs in the enterprise infrastructure—commonly referred to as an Administrative VLAN. Limit or block BMC access to the internet. If the BMC requires internet access to update, create rules such that only update-supporting traffic is permitted during the update download [CPG 2.F, 2.X].

3. Harden configurations

Consult vendor guides and recommendations for hardening BMCs against unauthorized access and persistent threats. UEFI hardening configuration guidance may apply to many BMC settings [CPG 1.E, 2.V, 2.W, 2.X]. [3]

4. Perform routine BMC update checks

BMC updates are delivered separately from most other software and firmware updates. Establish a routine to conduct monthly or quarterly checks for BMC updates according to the system vendor's recommendations and scheduled patch releases. Combine BMC update installations with routine server maintenance and scheduled downtime when possible. Note that some servers require a restart after BMC updates, while some can restart the BMC independent

of the OS or VMM. BMC updates may be provided via the internet, a local executable, an image stored on removable media, or network file storage [CPG 1.E].

Remember: OS patch maintenance solutions do not deliver BMC updates.

5. Monitor BMC integrity

Some BMCs report integrity data to a root of trust (RoT). The RoT could take the form of a TPM, dedicated security chip or coprocessor (multiple trademarked names in use), or a central processing unit (CPU) secure memory enclave. Monitor integrity features for unexpected changes and platform alerts [CPG 2.T].

6. Move sensitive workloads to hardened devices

Older server and cloud nodes may lack any BMC integrity monitoring mechanism. The presence of a TPM does not guarantee that BMC integrity data is collected. Place sensitive workloads on hardware designed to audit both the BMC firmware and the platform firmware [CPG 2.L].

7. Use firmware scanning tools periodically

Some modern EDR and platform scanning tools support BMC firmware capture. Establish a schedule to collect and inspect BMC firmware for integrity and unexpected changes. Include firmware audits in comprehensive anti-malware scanning tasks.

8. Do not ignore BMCs

A user may accidentally connect and expose an ignored and disconnected BMC to malicious content. Treat an unused BMC as if it may one day be activated. Apply patches. Harden credentials. Restrict network access. If a BMC cannot be disabled or removed, carry out recommended actions appropriate to the sensitivity of the platform's data [CPG 1.E, 2.C, 2.F, 2.K, 2.W, 2.X].

Works cited

[1] Eclypsium Inc. (2022), "The iLOBleed Implant: Lights Out Management Like You Wouldn't Believe." https://eclypsium.com/2022/01/12/the-ilobleed-implant-lights-out-management-like-you-wouldnt-believe

[2] National Institute of Standards and Technology (NIST) (2020), Special Publication 800-63B "Digital Identity Guidelines: Authentication and Lifecycle Management." https://pages.nist.gov/800-63-3/sp800-63b.html

[3] National Security Agency (NSA) (2018), "UEFI Defensive Practices Guidance." https://www.nsa.gov/portals/75/documents/what-we-do/cybersecurity/professional-resources/ctr-uefi-defensive-practices-guidance.pdf

Disclaimer of endorsement

The information and opinions contained in this document are provided "as is" and without any warranties or guarantees. Reference herein to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favoring by the United States Government, and this guidance shall not be used for advertising or product endorsement purposes.

Purpose

This document was developed in furtherance of the authoring agencies' cybersecurity missions, including their responsibilities to identify and disseminate threats and to develop and issue cybersecurity specifications and mitigations. This information may be shared broadly to reach all appropriate stakeholders.

Contact

Cybersecurity Report Feedback: CybersecurityReports@nsa.gov
General Cybersecurity Inquiries: Cybersecurity_Requests@nsa.gov
Defense Industrial Base Inquiries and Cybersecurity Services: DIB_Defense@cyber.nsa.gov
CISA's 24/7 Operations Center to report incidents and anomalous activity: Report@cisa.gov or (888) 282-0870
Media Inquiries / Press Desk:

- NSA Media Relations: 443-634-0721, MediaRelations@nsa.gov
- CISA Media Relations: 703-235-2010, CISAMedia@cisa.dhs.gov