Actively exploited vulnerability gives extraordinary control over server fleets



On Wednesday, CISA added CVE-2024-54085 to its list of vulnerabilities known to be exploited in the wild. The notice provided no further details.

In an email on Thursday, Eclypsium researchers said the scope of the exploits has the potential to be broad. That scope includes:

- *Attackers could chain multiple BMC exploits to implant malicious code directly into the BMC's firmware, making their presence extremely difficult to detect and allowing them to survive OS reinstalls or even disk replacements.*
- *By operating below the OS, attackers can evade endpoint*

protection, logging, and most traditional security tools.

- *With BMC access, attackers can remotely power on or off, reboot, or reimage the server, regardless of the primary operating system's state.*
- *Attackers can scrape credentials stored on the system, including those used for remote management, and use the BMC as a launchpad to move laterally within the network*
- *BMCs often have access to system memory and network interfaces, enabling attackers to sniff sensitive data or exfiltrate information without detection*
- *Attackers with BMC access can intentionally corrupt firmware, rendering servers unbootable and causing significant operational disruption*

With no publicly known details of the ongoing attacks, it's unclear which groups may be behind them. Eclypsium said the most likely culprits would be espionage groups working on behalf of the Chinese government. All five of the specific APT groups Eclypsium named have a history of exploiting firmware vulnerabilities or gaining persistent access to high-value targets.

Eclypsium said the line of vulnerable AMI MegaRAC devices uses an interface known as Redfish. Server makers known to use these products include AMD, Ampere Computing, ASRock, ARM, Fujitsu, Gigabyte, Huawei, Nvidia, Supermicro, and Qualcomm. Some, but not all, of these vendors have released patches for their wares.

Given the damage possible from exploitation of this vulnerability, admins should examine all BMCs in their fleets to ensure they aren't vulnerable. With products from so many different server makers affected, admins should consult with their manufacturer when unsure if their networks are exposed.

https://arstechnica.com/security/2025/06/active-exploitation-o

f-ami-management-tool-imperils-thousands-of-servers/