Vulnerabilities in Supermicro BMCs could allow for unkillable server rootkits

Getty Images

reader comments

32 with

If your organization uses servers that are equipped with baseboard management controllers from Supermicro, it may be time, once again, to patch seven high-severity vulnerabilities that attackers could exploit to gain control of them. And sorry, but the fixes must be installed manually.

Typically abbreviated as BMCs, baseboard management controllers are small chips that are soldered onto the motherboard of servers inside data centers. Administrators rely on these powerful controllers for various remote management capabilities, including installing updates, monitoring temperatures and setting fan speeds accordingly, and reflashing the UEFI system firmware that allows servers to load their operating systems during reboots. BMCs provide these capabilities and more, even when the servers they're connected to are turned off.

Code execution inside the BMC? Yup

The potential for vulnerabilities in BMCs to be exploited and used to take control of servers hasn't been lost on hackers. In 2021, hackers exploited a vulnerability in BMCs from HP Enterprise and installed a custom rootkit, researchers from

Amnpardaz, a security firm in Iran, reported that year. ILObleed, as the researchers named the rootkit, hid inside the iLO, a module in HPE BMCs that's short for Integrated Lights-Out.

ILObleed was programmed to destroy data stored on disk. If admins reinstalled the operating system, iLObleed would remain intact and reactivate the disk-wiping attack repeatedly. The unknown attackers responsible took control of the BMCs by exploiting a vulnerability HPE had fixed four years earlier. In June, the National Security Agency urged admins to follow guidance to prevent such incidents.

Researchers from security firm Binarly on Tuesday disclosed seven high-severity vulnerabilities in the IPMI (Intelligent Platform Management Interface) firmware for older Supermicro BMCs. Supermicro said in an advisory that the vulnerabilities affect "select X11, H11, B11, CMM, M11, and H12 motherboards." The advisory also thanked Binarly and provided patching information. There's no automated way to install the updates. Supermicro said it's unaware of any malicious exploitation of the vulnerabilities in the wild.

One of the seven vulnerabilities, tracked as CVE-2023-40289, allows for the execution of malicious code inside the BMC, but there's a catch: Exploiting the flaw requires already obtained administrative privileges in the web interface used to configure and control the BMCs. That's where the remaining six vulnerabilities come in. All six of them allow cross-site scripting, or XSS, attacks on machines used by admins. The exploit scenario is to use one or more of them in combination with CVE-2023-40289.

Advertisement
In an email, Binarly founder and CEO Alex Matrosov wrote:

> *Exploiting this vulnerability requires already obtained administrative privileges in the BMC Web Interface. To*

> *achieve it, a potential attacker can utilize any of the XSS vulnerabilities we found. In such a case, the exploitation path will look like this potential scenario:*
>
> *1. an attacker prepares a malicious link with the malicious payload*
> *2. includes it in phishing emails (for example)*
> *3. when this click is opened, the malicious payload will be executed inside BMC OS.*

Admins can remotely communicate with Supermicro BMCs through various protocols, including SSH, IPMI, SNMP, WSMAN, and HTTP/HTTPS. The vulnerabilities Binarly discovered can be exploited using HTTP. While the NSA and many other security practitioners strongly urge that BMC interfaces be isolated from the Internet, there's evidence that this advice is routinely ignored. A recent query to the Shodan search engine revealed more than 70,000 instances of Supermicro BMC that have their IPMI web interface publicly available.

Enlarge / A screenshot showing Shodan results.

The road map for exploiting the vulnerabilities against servers with Supermicro interfaces exposed this way is illustrated below:

Enlarge / The road map for exploiting a BMC that has its web interface exposed to the Internet.

In Tuesday's post, Binarly researchers wrote:

> *First, it is possible to remotely compromise the BMC system by exploiting vulnerabilities in the Web Server component exposed to the Internet. An attacker can then gain access to the Server's operating system via legitimate iKVM remote control BMC functionality or by flashing the UEFI of the target system with malicious firmware that allows persistent control of the host OS. From there, nothing prevents an attacker from lateral movement within the internal network, compromising other internal hosts.*

All the vulnerabilities Binarly discovered originate in IPMI firmware third-party developer ATEN developed for Supermicro. While ATEN patched CVE-2023-40289 six months ago, the fix never made its way into the firmware.

"This is a supply chain problem because it can be other BMC vendors that can be potentially impacted by these vulnerabilities," Matrosov wrote.

https://arstechnica.com/?p=1973415