Firmware vulnerabilities in millions of computers could give hackers superuser status

reader comments

39 with

Two years ago, ransomware crooks breached hardware-maker Gigabyte and dumped more than 112 gigabytes of data that included information from some of its most important supply-chain partners, including Intel and AMD. Now researchers are warning that the leaked information revealed what could amount to critical zero-day vulnerabilities that could imperil huge swaths of the computing world.

The vulnerabilities reside inside firmware that Duluth, Georgia-based AMI makes for BMCs (baseboard management controllers). These tiny computers soldered into the motherboard of servers allow cloud centers, and sometimes their customers, to streamline the remote management of vast fleets of computers. They enable administrators to remotely reinstall OSes, install and uninstall apps, and control just about every other aspect of the system—even when it's turned off. BMCs provide what's known in the industry as "lights-out" system management.

Lights-out forever

Researchers from security firm Eclypsium analyzed AMI firmware leaked in the 2021 ransomware attack and identified

vulnerabilities that had lurked for years. They can be exploited by any local or remote attacker with access to an industry-standard remote-management interface known as Redfish to execute malicious code that will run on every server inside a data center.

Until the vulnerabilities are patched using an update AMI published on Thursday, they provide a means for malicious hackers—both financially motivated or nation-state sponsored—to gain superuser status inside some of the most sensitive cloud environments in the world. From there, the attackers could install ransomware and espionage malware that runs at some of the lowest levels inside infected machines. Successful attackers could also cause physical damage to servers or indefinite reboot loops that a victim organization can't interrupt. Eclypsium warned such events could lead to "lights out forever" scenarios.

In a post published Thursday, Eclypsium researchers wrote:

> *These vulnerabilities range in severity from **High to Critical**, including **unauthenticated remote code execution and unauthorized device access with superuser permissions**. They can be exploited by remote attackers having access to Redfish remote management interfaces, or from a compromised host operating system. 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 often used in modern hyperscale environments.*
>
> *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 be passed 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. They can also impact upstream suppliers to organizations and should be discussed with key 3rd parties as part of general supply chain risk management due diligence.*
>
> *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 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 service infrastructure. The same logic flaws may affect devices in fall-back data centers in different geographic regions part of the same service provider, and can challenge assumptions cloud providers (and their customers) often make in the context of risk management and continuity of operations.*

The researchers went on to note that if they could locate the vulnerabilities and write exploits after analyzing the publicly available source code, there's nothing stopping malicious actors from doing the same. And even without access to the source code, the vulnerabilities could still be identified by decompiling BMC firmware images. There's no indication malicious parties have done so, but there's also no way to know they haven't.

Advertisement

The researchers privately notified AMI of the vulnerabilities, and the company created firmware patches, which are available to customers through a restricted support page. AMI has also published an advisory here.

The vulnerabilities are:

- CVE-2023-34329, an authentication bypass via HTTP headers that has a severity rating of 9.9 out of 10, and

- CVE-2023-34330, Code injection via Dynamic Redfish Extension. Its severity rating is 8.2.

https://arstechnica.com/?p=1955540