New Supermicro BMC flaws can create persistent backdoors

Data: 2025-09-24 21:54:41

Autor: Inteligência Against Invaders

Two vulnerabilities affecting the firmware of Supermicro hardware, includingBaseboard Management

Controller (BMC) allow attackers to update systems with maliciously craftedimages.

Supermicro is a maker of servers, motherboards, and data center hardware. BMCis a microcontroller on Supermicro server motherboards that permits remote system monitoring and management even if the system is powered off.

Experts at firmware security company Binarly discovered a bypass for a flaw (CVE-2024-10237) that Supermicro patched this year in January along with another vulnerabililty identified asCVE-2025-6198.

“This security issue could allow potential attackers to gain complete and persistent control of both the BMC system and the main server OS,” Binarly researchers say.

Both security issues can be used to update BMC systemswith unofficial firmware, but the researchers say thatCVE-2025-6198 can alse be exploited tobypass the BMC RoT (Root of Trust) – a security feature validating that the system is booting with legitimate firmware.

Planting malicious firmware enables persistence across reboots and OS re-installs, high-level control of the server, and reliable bypass of security checks.

To fix CVE-2024-10237, Supermicro added checks to restrict custom *fwmap* entries, which are a table of instructions inside the firmware image that could be leveraged to manipulate firmware images.

[IMAGEM REMOVIDA]discovered that it wasstill possible to inject a malicious *fwmap* before the vendor’s original is loaded by the system, declaring the signed regions in a way that would let the attacker relocate or replace actual content while keeping the digest consistent.

This means that the calculated hash equals the signed value and the signature verification succeeds, even though parts in the firmware image have been swapped or replaced.

[IMAGEM REMOVIDA]CVE-2025-7937.

The second bug that Binarly discovered,CVE-2025-6198, arises from a flawed validation logic within the *auth_bmc_sig* function, executed in the OP-TEE environment of the X13SEM-F motherboard firmware.

Since the signed regions are defined in the uploaded image itself, attackers can modify the kernel or other regions and relocate original data to unused firmware space, keeping the digest valid.

The researchers demonstrated flashing and execution of a customized kernel, demonstrating that kernel authentication is not performed during boot, meaning the Root of Trust feature only partially protects the process.

Bill Toulas

Bill Toulas is a tech writer and infosec news reporter with over a decade of experience working on various online publications, covering open-source, Linux, malware, data breach incidents, and hacks.

You may also like: