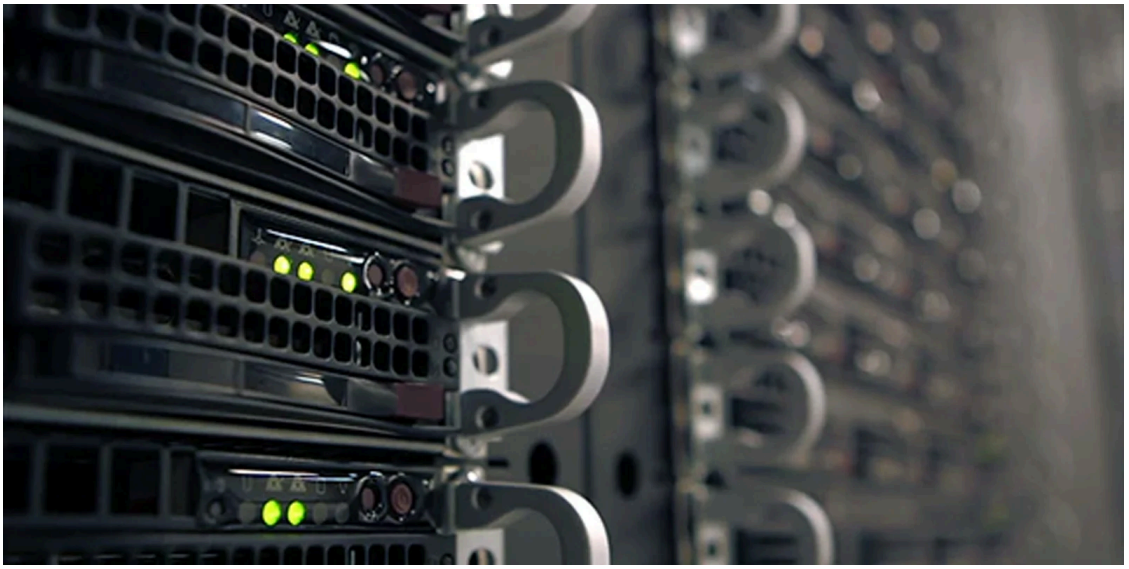
Supermicro, Pulse Secure release fixes for 'TrickBoot' attacks

By Lawrence Abrams

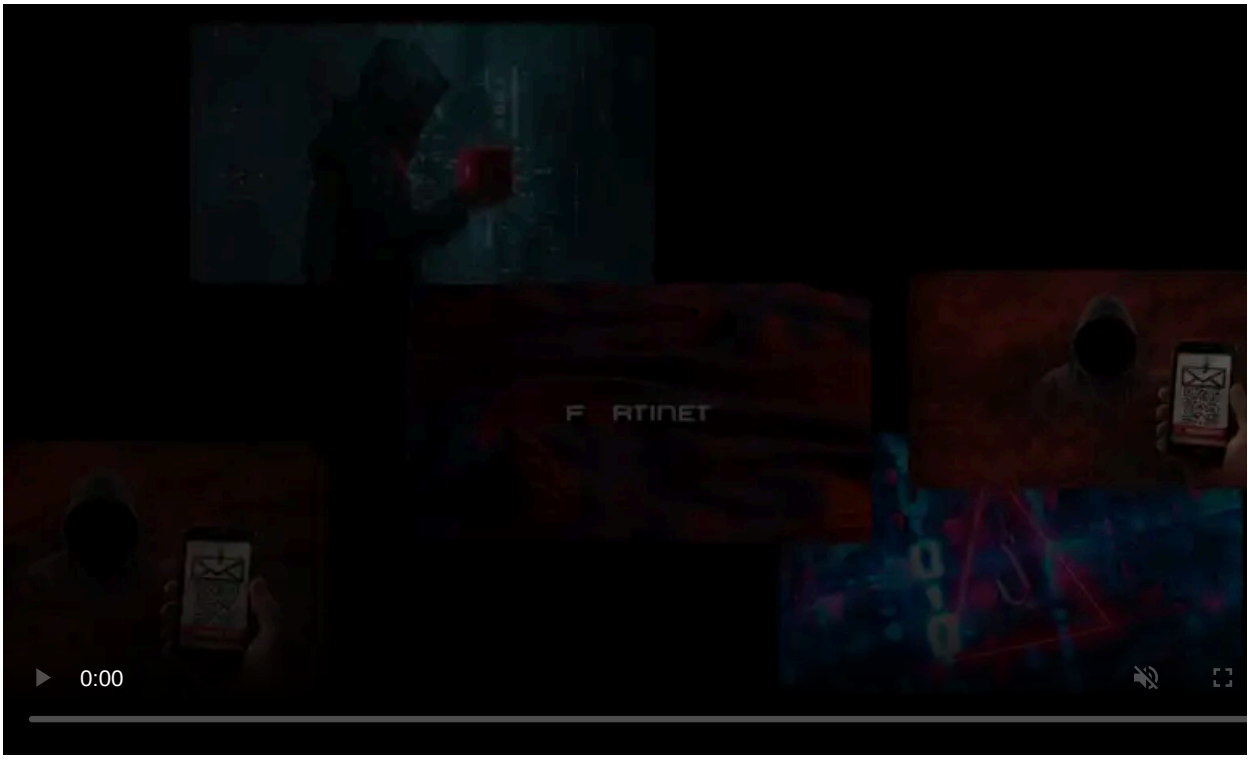
Published: 2021-03-05 · Archived: 2026-04-05 22:21:36 UTC

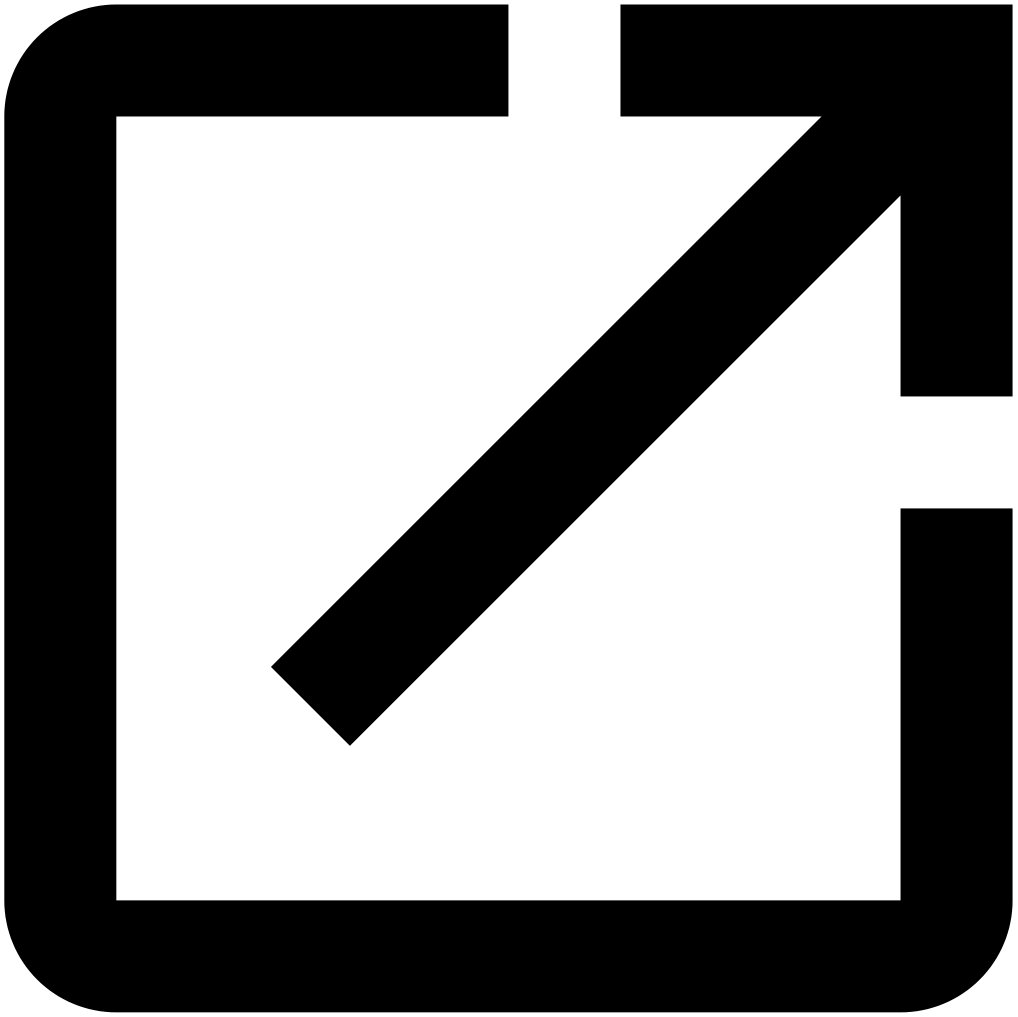


Supermicro and Pulse Secure have released advisories warning that some of their motherboards are vulnerable to the TrickBot malware's UEFI firmware-infecting module, known as TrickBoot.

Last year, cybersecurity firms Advanced Intelligence and Eclypsium released a joint report about a new malicious firmware-targeting 'TrickBoot' module delivered by the notorious TrickBot malware.

When executed, the module will analyze a device's UEFI firmware to determine if it has 'write protection' disabled. If it is, the malware contains the functionality to read, write, and erase the firmware.


F RTINET
0:00



This could allow the malware to perform various malicious activities, such as bricking a device, bypassing operating system security controls, or reinfecting a system even after a full reinstall.

To check if a UEFI BIOS has 'write protection' enabled, the module uses the RwDrv.sys driver from the RWEverything utility.

> "All requests to the UEFI firmware stored in the SPI flash chip go through the SPI controller, which is part of the Platform Controller Hub (PCH) on Intel platforms. This SPI controller includes access control mechanisms, which can be locked during the boot process in order to prevent unauthorized modification of the UEFI firmware stored in the SPI flash memory chip.
>
> Modern systems are intended to enable these BIOS write protections to prevent the firmware from being modified; however, these protections are often not enabled or misconfigured. If the BIOS is not write-protected, attackers can easily modify the firmware or even delete it completely," Eclypsium and Advanced Intel.

The malware's ability to analyze a device's firmware is currently restricted to specific Intel platforms, including Skylake, Kaby Lake, Coffee Lake, Comet Lake.

Supermicro, Pulse Secure release advisories

In an advisory released today, Supermicro is warning that some of their X10 UP motherboards are vulnerable to the TrickBoot malware and have released a 'critical' BIOS update to enable write protection.

"Supermicro is aware of the **Trickboot** issue which is observed only with a **subset of the X10 UP motherboards**. Supermicro will be providing a mitigation for this vulnerability," Supermicro warned today in a security advisory.

The vulnerable X10 UP-series ("**Denlow**") motherboards are listed below.

1. **X10SLH-F** (will EOL on 3/11/2021)
2. **X10SLL-F** (EOL'ed since 6/30/2015)
3. **X10SLM-F** (EOL'ed since 6/30/2015)
4. **X10SLL+-F** (EOL'ed since 6/30/2015)
5. **X10SLM+-F** (EOL'ed since 6/30/2015)
6. **X10SLM+-LN4F** (EOL'ed since 6/30/2015)
7. **X10SLA-F** (EOL'ed since 6/30/2015)
8. **X10SL7-F** (EOL'ed since 6/30/2015)
9. **X10SLL-S**/**-SF** (EOL'ed since 6/30/2015)

Supermicro has released BIOS version 3.4 to fix the vulnerability but has only released it publicly for the X10SLH-F motherboard.

For those motherboards that have reached the end of life, owners must contact Supermicro to get access to the new BIOS.

Pulse Secure also issued an advisory as their Pulse Secure Appliance 5000 (PSA-5000), and Pulse Secure Appliance 7000 (PSA-7000) devices run on vulnerable Supermicro hardware.

At this time, Pulse Secure has released a BIOS patch for devices running Pulse Connect Secure or Pulse Policy Secure. Pulse One (On-Prem Appliance Only) owners will have to wait a bit longer for a patch to be released.

Pulse Secure warns that apply the patch will require a reboot of the device.
