Detected a security flaw in Lenovo's UEFI firmware, affecting 100 laptop models

Users who are using affected laptop models should update to the latest firmware to be on the safe side.

Lenovo has just published a security advisory about vulnerabilities affecting Unified Extensible Firmware Interface (UEFI) installed on at least 100 of its laptop models.

A total of 3 security issues were discovered, two of which allowed hackers to disable protection for SPI flash memory chips, where UEFI firmware is stored, and disable UEFI Secure Boot, which ensures that at At startup the computer loads only code that is trusted by the OEM.

If successfully exploiting the third vulnerability, CVE-2021-3970, hackers can execute arbitrary code with elevated privileges.

All three vulnerabilities were responsibly discovered by ESET researchers and reported to Lenovo last year. They affect more than 100 consumer laptop models including the IdeaPad 3, Legion 5 Pro-16ACH6 H, Yoga Slim 0-14ITL05. This equates to millions of users using vulnerable devices.

Installed the wrong driver

Researchers at ESET warn that two UEFI-related vulnerabilities (CVE-2021-3971 and CVE-2021-3972) can be used by hackers to successfully deploy and execute SPI flash or ESP implants.

Both UEFI-related security problems in Lenovo products stem from two drivers being installed by mistake. Specifically, drivers named SecureBackDoor and SecureBackDoorPeim, which were only used in the production

process, were mistakenly installed on commercial devices.

It is very difficult to detect UEFI with malicious code

According to ESET, UEFI-related threats are often very dangerous and difficult to detect. This is because they execute early in the boot process before transferring control to the operating system.

This means that all mitigations and security solutions that work at the executive level are useless and the implicit execution of payloads is inevitable and undetectable.

Of course, it is still possible to detect this type of attack, but it will require more advanced techniques such as UEFI integrity checking, real-time firmware analysis or device and firmware behavior monitoring to detect this type of attack. Look for suspicious activity.

Security companies have identified two such implantation attacks in the past, both of which are used by hackers in actual attacks:

1. Lojax - discovered in 2018 and used by Russian state-sponsored hackers such as APT28, Fancy Bear, Sednit, Strontium and Sofacy.
2. ESPcter - discovered in 2021 and active since 2012.

However, this is not the only UEFI threat detected. Kasspersky has published reports on MosaicRegressor in 2020, FinSpy in 2021, and MoonBounce in January 2022.

To be safe from attacks from these vulnerabilities, Lenovo recommends that affected laptop users update the firmware to the latest version available.

This can be done by downloading and installing it manually from the device's support page or with the help of system driver update utilities provided by Lenovo.