Vulnerabilities allowing permanent infections affect 70 Lenovo laptop models

reader comments

30 with 26 posters participating

Share this story

For owners of more than 70 Lenovo laptop models, it’s time once again to patch the UEFI firmware against critical vulnerabilities that attackers can exploit to install malware that’s nearly impossible to detect or remove.

The laptop maker on Tuesday released updates for three vulnerabilities that researchers found in the UEFI firmware used to boot up a host of its laptop models, including the Yoga, ThinkBook, and IdeaPad lines. The company assigned a medium severity rating to the vulnerabilities, which are tracked CVE-2022-1890, CVE-2022-1891, and CVE-2022-1892 and

affect the ReadyBootDxe, SystemLoadDefaultDxe, and SystemBootManagerDxe drivers, respectively.

“The vulnerabilities can be exploited to achieve arbitrary code execution in the early phases of the platform boot, possibly allowing the attackers to hijack the OS execution flow and disable some important security features,” security firm ESET said. “These vulnerabilities were caused by insufficient validation of DataSize parameter passed to the UEFI Runtime Services function GetVariable. An attacker could create a specially crafted NVRAM variable, causing buffer overflow of the Data buffer in the second GetVariable call.”

> *The vulnerabilities can be exploited to achieve arbitrary code execution in the early phases of the platform boot, possibly allowing the attackers to hijack the OS execution flow and disable some important security features. 2/6*
>
> *— ESET research (@ESETresearch) July 13, 2022*

Short for Unified Extensible Firmware Interface, UEFI is the software that bridges a computer’s device firmware with its operating system. As the first piece of software to run when virtually any modern machine is turned on, it’s the first link in the security chain. Because the UEFI resides in a flash chip on the motherboard, infections are difficult to detect and remove. Typical measures such as wiping the hard drive and reinstalling the OS have no meaningful impact because the UEFI infection will simply reinfect the computer afterward.

Many motherboard-resident flash chips that store the UEFI have access control mechanisms that can be locked during the boot process to prevent unauthorized firmware changes. It’s not clear if the affected Lenovo models have that capability. Even if they do, these protections are often turned off, misconfigured, or hampered by vulnerabilities. ESET researchers weren’t immediately available to comment on the

requirements for exploits of these particular vulnerabilities.

In any event, owners of Lenovo laptops should take a minute to check Wednesday’s advisory to see if their model is vulnerable since firmware updates often require manual installation.

https://arstechnica.com/?p=1866641