Microsoft will take nearly a year to finish patching new 0-day Secure Boot bug

reader comments

86 with

Earlier this week, Microsoft released a patch to fix a Secure Boot bypass bug used by the BlackLotus bootkit we reported on in March. The original vulnerability, CVE-2022-21894, was patched in January, but the new patch for CVE-2023-24932 addresses another actively exploited workaround for systems running Windows 10 and 11 and Windows Server versions going back to Windows Server 2008.

The BlackLotus bootkit is the first-known real-world malware that can bypass Secure Boot protections, allowing for the execution of malicious code before your PC begins loading Windows and its many security protections. Secure Boot has been enabled by default for over a decade on most Windows PCs sold by companies like Dell, Lenovo, HP, Acer, and others. PCs running Windows 11 must have it enabled to meet the software's system requirements.

Microsoft says that the vulnerability can be exploited by an attacker with either physical access to a system or administrator rights on a system. It can affect physical PCs and virtual machines with Secure Boot enabled.

We highlight the new fix partly because, unlike many high-priority Windows fixes, the update will be disabled by default

for at least a few months after it’s installed and partly because it will eventually render current Windows boot media unbootable. The fix requires changes to the Windows boot manager that can’t be reversed once they’ve been enabled.

“The Secure Boot feature precisely controls the boot media that is allowed to load when an operating system is initiated, and if this fix is not properly enabled there is a potential to cause disruption and prevent a system from starting up,” reads one of several Microsoft support articles about the update.

Additionally, once the fixes have been enabled, your PC will no longer be able to boot from older bootable media that doesn’t include the fixes. On the lengthy list of affected media: Windows install media like DVDs and USB drives created from Microsoft’s ISO files; custom Windows install images maintained by IT departments; full system backups; network boot drives including those used by IT departments to troubleshoot machines and deploy new Windows images; stripped-down boot drives that use Windows PE; and the recovery media sold with OEM PCs.

Advertisement

Not wanting to suddenly render any users’ systems unbootable, Microsoft will be rolling the update out in phases over the next few months. The initial version of the patch requires substantial user intervention to enable—you first need to install May’s security updates, then use a five-step process to manually apply and verify a pair of “revocation files” that update your system’s hidden EFI boot partition and your registry. These will make it so that older, vulnerable versions of the bootloader will no longer be trusted by PCs.

A second update will follow in July that won’t enable the patch by default but will make it *easier* to enable. A third update in “first quarter 2024” will enable the fix by default and render older boot media unbootable on all patched Windows

PCs. Microsoft says it is “looking for opportunities to accelerate this schedule,” though it’s unclear what that would entail.

Jean-Ian Boutin, ESET’s director of threat research, described the severity of BlackLotus and other bootkits to Ars when we originally reported on it:

> *The ultimate takeaway is that UEFI bootkit BlackLotus is able to install itself on up-to-date systems using the latest Windows version with secure boot enabled. Even though the vulnerability is old, it is still possible to leverage it to bypass all security measures and compromise the booting process of a system, giving the attacker control over the early phase of the system startup. It also illustrates a trend where attackers are focusing on the EFI System Partition (ESP) as opposed to firmware for their implants—sacrificing stealthiness for easier deployment—but allowing a similar level of capabilities.*

This fix isn’t the only recent security incident to highlight the difficulties of patching low-level Secure Boot and UEFI vulnerabilities; computer and motherboard maker MSI recently had its signing keys leaked in a ransomware attack, and there’s no simple way for the company to tell its products not to trust firmware updates signed with the compromised key.

https://arstechnica.com/?p=1938719