Eclypsium security report shows unsigned firmware as ongoing headache

February 20 2020, by Nancy Cohen

Credit: CC0 Public Domain

Risky business has an impact on computer users and known brand-name vendors, and it is all about firmware, rarely scanned for vulnerabilities, and which can subvert existing security controls. A new report from

enterprise firmware security company Eclypsium reports on Windows and Linux firmware vulnerabilities.

In its PR materials, Eclypsium says, "Modern attackers know that traditional security tools lack visibility into firmware, both at the system level and within hardware components, and are increasingly using firmware implants and backdoors to bypass security controls, persist and disrupt an organization's infrastructure."

These developments turn a lot of security assumptions upside-down, as many security technologies are bypassed. The Eclypsium report team saw how "peripheral devices often lack the same security best practices that we take for granted in operating systems and in other more visible components, like the UEFI or BIOS."

In a Wired story, Rick Althert, principal engineer at Eclypsium, said unprivileged users can modify firmware on these devices; there are no checks regarding where that firmware came from or what it does.

Other technology sites also put the new report, "Perilous Peripherals: The Hidden Dangers Inside Windows and Linux Computers," in the spotlight.

Brand names with firmware weaknesses include Lenovo, HP and Dell peripherals. The report said they found unsigned firmware in WiFi adapters, USB hubs, trackpads and cameras used in computers from Lenovo, Dell, HP and other major manufacturers. The firmware could be updated with unsigned code.

Tara Seals at Threatpost said that firmware could provide criminals "with a rich attack surface if found to be vulnerable."

Shaun Nichols wrote in The Register, "while the vulnerable devices

themselves may not be particularly valuable to a hacker, they can serve as a foothold for getting into other systems on the network."

The report team said that "unsigned firmware can lead to the loss of data, integrity, and privacy, and can allow attackers to gain privileges and hide from traditional security controls."

Advice from Eclypsium: "Given the widespread nature of unsigned firmware, enterprises should scan their devices for any vulnerable components, and should assess the firmware posture of new devices during procurement."

Firmware vulnerabilities can be hard to detect. Seals wrote that firmware attacks "allow malicious activity to fly under the radar of endpoint protections, as recently seen in the latest campaigns using the RobbinHood ransomware, vulnerable drivers can be used to bypass security protections and enable ransomware to attack without interference."

Of all the reports on what Eclypsium bared, Andy Greenberg's article was especially helpful for those who need to better understand how peripherals can mess with a user's security.

"That laptop on your desk or that server on a data center rack isn't so much a computer as a network of them. Its interconnected devices—from hard drives to webcams to trackpads, largely sourced from third parties—have their own dedicated chips and code."

Never mind that warnings have been issued for years—the problem persists. Greenberg said, "Those computers inside your computer remain disturbingly unprotected."

The researchers even found issues with the Linux Vendor Firmware

Service, "a secure portal that allows hardware vendors to upload firmware updates."

The bottom line in the Threatpost article was that this firmware problem is hardly trivial. "Unsigned firmware in peripheral devices remains a highly overlooked aspect of cybersecurity," wrote Seals, "and provides multiple pathways for malicious actors to compromise laptops and servers."

Paul Wagenseil at Tom's Guide had a similar point about its seriousness: "Millions of laptops and desktops made by Dell, HP, Lenovo and other companies are vulnerable to attack, thanks to unsecured firmware used by the webcams, trackpads, USB hubs, Wi-Fi cards and other peripheral devices from third-party suppliers that are built into the PCs."

Seals quoted Jesse Michaels, principal researcher at Eclypsium. He said that peripheral manufacturers have been slow to adopt the practice of signing firmware, "leaving millions of Windows and Linux systems at risk of firmware attacks that can exfiltrate data, disrupt operations and deliver ransomware."

Tom's Guide: "Microsoft can harden Windows, and Linux developers can harden Linux, against malware all they can, but operating system improvements won't do much to stop other lines of attack through the hundreds of third-party peripherals built into laptops and desktops."

Eclypsium's researchers found that these issues apply to virtually all classes of Windows and Linux devices, from laptops to servers. If it was unclear who to blame, it was also clear by Wednesday that one entity could be praised: Apple. "Macs are immune," said Tom's Guide.

The Eclypsium report explained that "Apple performs signature verification on all files in a driver package, including firmware, each

time before they are loaded into the device to mitigate this type of attack. In contrast, Windows and Linux only perform this type of verification when the package is initially installed."

A reader at HotHardware responded to the news with this viewpoint:

"There's really no excuse for any firmware to not be signed and verified anymore, outside of a development environment. Operating systems should prompt users with warnings about unsigned firmware and explain the dangers in a way lay users can understand. In enterprise environments, these warnings could be turned off via GPO, etc. presuming the SysAdmins are competent enough to vet their own firmware."

More information: eclypsium.com/2020/2/18/unsign … peripheral-firmware/

© 2020 Science X Network

Citation: Eclypsium security report shows unsigned firmware as ongoing headache (2020, February 20) retrieved 1 May 2024 from https://techxplore.com/news/2020-02-eclypsium-unsigned-firmware-ongoing-headache.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.