More than 40 Windows drivers contain dangerous privilege escalation vulnerabilities

There are more than 40 different drivers containing vulnerabilities that contain holes or poor code that can be exploited by hackers ...

Researchers from the Eclypsium network security company recently announced a shocking disclosure, that there are more than 40 different drivers, derived from 20 hardware vendors certified by Microsoft. Receiving or hiding vulnerabilities or poor code can be exploited by hackers to conduct privileged escalation attacks, thereby hijacking remote systems.

Specifically in DEF CON 2019, one of the biggest security - cyber security conferences of the year has just taken place in Las Vegas, the team of researchers from Eclypsium has published a list of 'solid'. BIOS vendors are also affected by hardware manufacturing units, including the names that are making up the largest market share such as ASUS, Huawei, Intel, NVIDIA and Toshiba.

1. Microsoft releases a new Windows 10 update, Microsoft Edge will be hidden if you install Edge Chromium

These drivers come from 20 hardware vendors that have been certified by Microsoft

Notably, these drivers are relevant and are used on nearly all current versions of Windows, which means millions of people around the world are at risk of becoming victims of attacks. Dangerous privilege escalation.

These drivers are capable of enabling malicious applications to gain kernel privileges at the user level, thereby gradually gaining direct access to the firmware and ultimately target hardware.

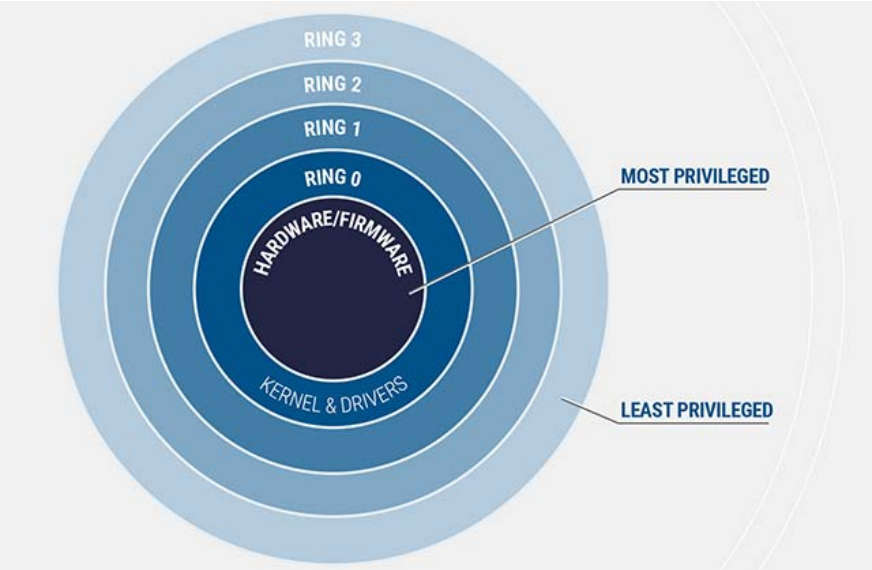
Also because malware can be installed directly into the firmware, so reinstalling the operating system is not a solution that can be effective in this case.

1. Windows Defender is one of the best antivirus applications in the world

All of the vulnerabilities found allow the driver to act as a proxy to enforce access with high privileges on hardware resources, such as being able to read and write data to the I / O space of processor and chipset (MSR), Model Specific Registers (MSR), Control Registers (CR), Debug Registers (DR), besides both physical memory and kernel virtual memory.

This is a privilege escalation because it can help an attacker switch from user mode (Ring 3) to kernel OS mode (Ring 0). The concept of protection rings is briefly described in the image illustrated below, in which the deeper inside will require more system privileges.

1. Choose which antivirus software to install on Windows 10 / 8.1 / 7 and this is Microsoft's recommendation



The protection rings in Windows, the deeper inside will require more system privileges

It is important to note that even ordinary system administrators only own the privileges to operate at Ring 3 (rarely enter deeper). The ability to access the kernel (Ring finally) can not only give attackers the highest level of access privilege available to the operating system, but can also help them own more access to the operating system. interface hardware and firmware with even higher privileges such as the system's BIOS firmware.

If a driver containing a vulnerable vulnerability is present on your system, the malicious application will only need to search for that driver name and exploit to raise privileges. Otherwise, if the driver containing the vulnerability does not exist in the system, the malicious application can still bring the driver for the error itself, but it needs an administrator's approval to install it now. these drivers.

'Driver not only provides the necessary privileges, but also possesses mechanisms to make changes'.

In a statement to ZDNet, Mickey Shkatov, a cyber security expert headed by the Eclypsium team, said:

"Microsoft will use the HVCI feature (Code Integrity) implemented by Hypervisor) for our blacklisted drivers."

However, this feature will only be available on 7th and newer Intel processors. HCVI will be disabled on older version CPUs, so if you want to uninstall faulty drivers, you will have to do it manually.

Besides, Microsoft also said:

"To exploit the vulnerability-prone drivers, hackers will first be forced to infiltrate the victim's computer."

Typically, attackers will invade the system at Ring 3 privilege level, then they will try to gain access to the kernel.

Security recommendations made by Microsoft are as follows:

1. Control the Windows Defender application to block vulnerable drivers and software.
2. Users can further protect themselves by activating memory integrity for devices that are likely to be hacked in under Windows Security.

1. What is Windows Core? Is it the future of Windows operating system?

Here is the complete book of all providers who have completed the driver update process:

1. ASRock
2. ASUSTeK Computer
3. ATI Technologies (AMD)
4. Biostar
5. EVGA
6. Getac
7. GIGABYTE
8. Huawei
9. Insyde
10. Intel
11. Micro-Star International (MSI)
12. NVIDIA
13. Phoenix Technologies
14. Realtek Semiconductor
15. SuperMicro
16. Toshiba