SCREWED DRIVERS— SIGNED, SEALED, DELIVERED

Common Design Flaw In Dozens of Device Drivers
Allows Widespread Windows Compromise

INTRODUCTION

As part of Eclypsium's ongoing hardware and firmware security research, we have become increasingly interested in the area of insecure drivers and how they can be abused in an attack against a device. Drivers that provide access to system BIOS or system components for the purposes of updating firmware, running diagnostics, or customizing options on the component can allow attackers to turn the very tools used to manage a system into powerful threats that can escalate privileges and persist invisibly on the host.

Recent research and attacks in the wild have made it clear that this area warrants additional scrutiny. For example, other research has revealed vulnerabilities in individual hardware vendor drivers (e.g. ASUS, ASRock, GIGABYTE) that allowed applications with user privileges to read and write with the privileges of kernel. This is obviously a serious escalation of privileges, and we wanted to know if these sorts of vulnerabilities were isolated incidents or examples of a more widespread problem. Secondly, there are multiple examples of attacks in the wild that take advantage of this class of vulnerable drivers. For example, the Slingshot APT campaign installs a kernel rootkit by exploiting drivers with read/write MSR capabilities in order to bypass driver signing enforcement. And the recent LoJax malware abused similar driver functionality to install malicious implants within the firmware of a victim device and persist even across a complete reinstallation of the operating system.

Our analysis found that the problem of insecure drivers is widespread, affecting more than 40 drivers from at least 20 different vendors - including every major BIOS vendor, as well as hardware vendors like ASUS, Toshiba, NVIDIA, and Huawei. However, the widespread nature of these vulnerabilities highlights a more fundamental issue - all the vulnerable drivers we discovered have been certified by Microsoft. Since the presence of a vulnerable driver on a device can provide a user (or attacker) with improperly elevated privileges, we have engaged Microsoft to support solutions to better protect against this class of vulnerabilities, such as blacklisting known bad drivers.

OVERVIEW AND IMPACT OF THE VULNERABILITIES

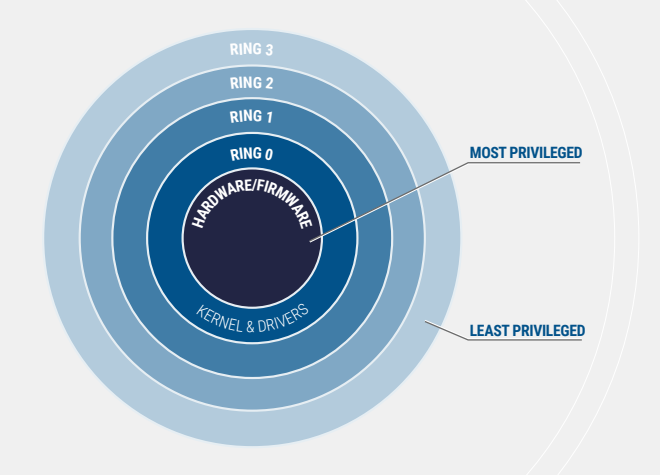
All these vulnerabilities allow the driver to act as a proxy to perform highly privileged access to the hardware resources, such as read and write access to processor and chipset I/O space, Model Specific Registers (MSR), Control Registers (CR), Debug Registers (DR), physical memory and kernel virtual memory. This is a privilege escalation as it can move an attacker from user mode (Ring 3) to OS kernel mode (Ring 0). The concept of protection rings is summarized in the image below, where each inward ring is granted progressively more privilege. It is important to note that even Administrators operate at Ring 3 (and no deeper), alongside other users. Access to the kernel can not only give an attacker the most privileged access available to the operating system, it can also grant access to the hardware and firmware interfaces with even higher privileges such as the system BIOS firmware.

HOW VULNERABILITIES CAN BE USED IN AN ATTACK

A vulnerable driver installed on a machine could allow an application running with user privileges to escalate to kernel privileges and abuse the functionality of the driver. In other words, any malware running in the user space could scan for a vulnerable driver on the victim machine and then use it to gain full control over the system and potentially the underlying firmware. However, if a vulnerable driver is **not** already on a system, administrator privilege would be required to install a vulnerable driver.

As mentioned earlier, a vulnerable driver could also give an attacker access to the "negative" firmware rings that lie beneath the operating system. As seen with the LoJax malware, this allows malware to attack vulnerable system firmware (e.g. UEFI) to maintain persistence on the device, even if the operating system is completely reinstalled. The problem extends to device components, in addition to the system firmware. Some vulnerable drivers interact with graphics cards, network adapters, hard drives, and other devices. Persistent malware inside these devices could read, write, or redirect data stored, displayed or sent over the network. Likewise, any of the components could be disabled as part of a DoS or ransomware attack.

Since many of the drivers themselves are designed to update firmware, the driver is providing not only the necessary privileges, but also the mechanism to make changes.



SIGNED AND CERTIFIED DOES NOT MEAN SAFE

It is of particular concern that the drivers in question were not rogue or unsanctioned - in fact, just the opposite. All the drivers come from trusted third-party vendors, signed by valid Certificate Authorities, and certified by Microsoft. Both Microsoft and the third-party vendors will need to be more vigilant with these types of vulnerabilities going forward.

These issues apply to all modern versions of Microsoft Windows and there is currently no universal mechanism to keep a Windows machine from loading one of these known bad drivers. Implementing group policies and other features specific to Windows Pro, Windows Enterprise and Windows Server may offer some protection to a subset of users. Once installed, these drivers can reside on a device for long periods of time unless specifically updated or uninstalled. In addition to the drivers which are already installed on the system, malware can bring any of these drivers along with them to perform privilege escalation and gain direct access to the hardware.

IMPACTS AND MITIGATION

The presence of vulnerable drivers can make it increasingly challenging to secure the firmware attack surface. Vulnerable or outdated system and component firmware is a common problem and a high value target for attackers, who can use it to launch other attacks, completely brick systems, or remain on a device for years gathering data, even after the device is wiped. To make matters worse, in this case, the very drivers and tools that would be used to update the firmware are themselves vulnerable and provide a potential avenue for attack. As a result, organizations should not only continuously scan for outdated firmware, but also update to the latest version of device drivers when fixes become available from device manufacturers.

Organizations may also want to keep their firmware up to date, scan for vulnerabilities, monitor and test the integrity of their firmware to identify unapproved or unexpected changes.

LIST OF AFFECTED VENDORS

- American Megatrends International (AMI)
- ASRock
- ASUSTeK Computer
- ATI Technologies (AMD)
- Biostar
- EVGA
- Getac
- GIGABYTE
- Huawei
- Insyde
- Intel
- Micro-Star International (MSI)
- NVIDIA
- Phoenix Technologies
- Realtek Semiconductor
- SuperMicro
- Toshiba

Some affected vendors are still under embargo due to their work in highly regulated environments and will take longer to have a fix certified and ready to deploy to customers.

You can read the Black Hat presentation here.