# UEFI firmware from Microsoft, Intel, HP, Dell etc., can be at risk from nearly 20 different vulnerabilities

Binarly, a security research company that specializes in dealing with firmware-related threats, revealed a very disturbing piece of information in a recent blog post.

That is the InsydeH2O "Hardware-2-Operating System" UEFI BIOS, a software used by a series of major vendors in the computer field such as Microsoft, Intel, HP, Dell, Lenovo, Siemens, Fujitsu, etc., can be affected by more than two dozen different vulnerabilities, with ratings ranging from common to dangerous.

According to Binarly's investigation results, there are a total of 23 vulnerabilities that mainly affect System Management Mode (SMM). Information about these vulnerabilities is listed below along with their assigned security IDs.

| Product | Processor | ARM core | Debian/Raspbian ARM port (maximum) | Architecture width |
|---|---|---|---|---|
| Raspberry Pi 1 | BCM2835 | ARM1176 | arm6hf | 32 bit |
| Raspberry Pi 2 | BCM2836 | Cortex-A7 | armhf | 32 bit |
| Raspberry Pi Zero | BCM2835 | ARM1176 | arm6hf | 32 bit |
| Raspberry Pi Zero 2 | BCM2710 | Cortex-A53 | arm64 | 64 bit |
| Raspberry Pi 3 | BCM2710 | Cortex-A53 | arm64 | 64 bit |
| Raspberry Pi 4 | BCM2711 | Cortex-A72 | arm64 | 64 bit |

Since these are all firmware-level vulnerabilities, successful exploitation can lead to persistent malware on the system that is almost impossible for users to completely remove.

Binarly describes the detected vulnerabilities as follows:

> The majority of disclosed vulnerabilities (CVSS score: 7.5 - 8.2, high severity rating) resulted in code execution with SMM privileges. As part of the exploit chain, these vulnerabilities can be used as a second stage in a malicious process, to bypass security features or achieve long-term survival on the target system. [.]
>
> By exploiting these vulnerabilities, attackers can successfully install malware that exists during the root of the operating system, and allows bypassing endpoint security solutions (EDRs). /AV), Secure Boot, Virtualization-Based Security.

The Binarly team first discovered these vulnerabilities on Fujitsu's LIFEBOOK notebook computers. After extensive investigation, it was quickly realized that not only Fujitsu, but also software from a variety of other manufacturers could be affected by these vulnerabilities. Cause because all are using InsydeH2O UEFI solutions.