Firmware, blind spots flagged by Spectre attack research

22 May 2018, by Nancy Owano

Credit: CC0 Public Domain

Software vulnerability discoveries by security researchers come and go and are more often than not promptly followed by vendor fixes. After each headline scare, you read the labs' reports, you hear about the fixes, and well, everyone can relax, for at least the moment.

Firmware news regarding vulnerabilities are another matter and worrying. That is why a Spectre finding is making news this month. A threat watcher who was once with Intel now heads firmware-attack monitoring Eclypsium and has reported new findings on vulnerabilities.

Bloomberg was among numerous sites reporting that Intel's former chief threat researcher found new vulnerabilities that build on the Spectre bugs. Such flaws were revealed by a former leader of Intel's advanced threat research team, Yuriy Bulygin, who is now CEO of Eclypsium.

The research showed it was possible to perform a hacker exploit to access a computer's firmware.

Bleeping Computer said the new variation of a Spectre attack recovers data from a CPU's protected SMM Mode. SMM stands for System Management Mode. It's an operating mode of x86 central processor units (CPUs). Catlin Cimpanu explained the attack can recover data stored inside a secure CPU area.

OSDev.org, a community of operating system developers, said the mode was "intended for use by Firmware/BIOS to perform low-level system management operations while an OS is running."

This new variant of Spectre can expose the contents of memory that normally cannot be accessed by the OS kernel, wrote Liam Tung, *ZDNet*.

Jordan Robertson in Bloomberg said, "With access to the SMM memory, hackers can get essentially any data they want."

Cimpanu said the SMM is a special x86 processor mode "that not even highly-privileged software such as kernels or hypervisors cannot access or interrupt." Cimpanu noted that "software applications of any kind are not allowed to interact with the SMM, for both maintenance and security reasons."

The attack can expose SMM code and data that was intended to be confidential.

Robertson in Bloomberg added that "hackers who access those systems' firmware can not only move between the databases and steal information but also look through the firmware's own code to reveal some of the servers' most heavily defended secrets, including encryption keys and administrative passwords."

Cimpanu said, "This is also not the first variation of the original Spectre vulnerability. Other Spectre-related attacks include SgxSpectre, BranchScope, and SpectrePrime."

So how did Eclypsium carry out the attack? Cimpanu said, on Intel CPUs, access to the SMM is protected by a type of range registers known as System Management Range Register (SMRR).

Well, the team found a way to bypass the SMRR mechanism. They could access data stored in the System Management RAM (SMRAM), and that, said Cimpanu, is the area where SMM runs its working data.

In the bigger picture, Bloomberg reflected on firmware. "Eclypsium is one of a handful of companies developing technology to look for malicious modifications to the firmware inside companies' data centers."

Elysium itself has pointed out that "Firmware in servers, laptops, and networking equipment has become the new target for adversaries who realize that this is a defender's blind spot."

Blind spot, in what way? Robertson said that this class of hardware attack was virtually undetectable. "Software hacks can usually be removed with a security update, but malicious code that makes its way into firmware could be there forever because of its role in the backbone of a chip or processor". He quoted Bulygin, who said it was "a blind spot with a huge attack surface." and that, Bulygin added, was "obviously not a good combination.'"

"The main motherboard, network cards, management controllers, storage devices and dozens of other components at the heart of our devices all rely on firmware developed by different manufacturers and can be compromised. This is true for any type of device and OS ranging from laptops to the servers that run our applications in enterprise, to the network appliances that operate our network infrastructure, to industrial systems that operate our critical infrastructure," said a post on Eclypsium. "It is a large attack surface and devices can be backdoored in the supply chain before you ever pull it out of the box.".

Rob Williams in *Hot Hardware* said that "If there's an upside to these new attack vectors, it's that Intel claims that mitigating Spectre variant 1 in effect takes care of this added SMM exploit."

Researchers had notified Intel of their new Spectre attack variation, said *Bleeping Computer*. "Intel says that the original patches for the Spectre variant 1 and variant 2 should be enough to block the attack chain discovered by the Eclypsium team."

Sure enough, Intel's statement, as reported on several sites, said, '"We have reviewed Eclypsium's research and, as noted in their blog, we believe that the existing guidance for mitigating Variant 1 and Variant 2 will be similarly effective at mitigating these scenarios," an Intel spokesperson said. "We value our partnership with the research community and are appreciative of Eclypsium's work in this area.'"

Moving forward, Williams had this to say: "all we can do is hope that future microprocessors are not going to suffer such a wide-reaching bug. AI could very-well help with this kind of thing, detecting issues long before a human does. We need that backup help sooner than later."