FLOOD OF NEW ADVISORIES EXPOSE MASSIVE GAPS IN FIRMWARE SECURITY

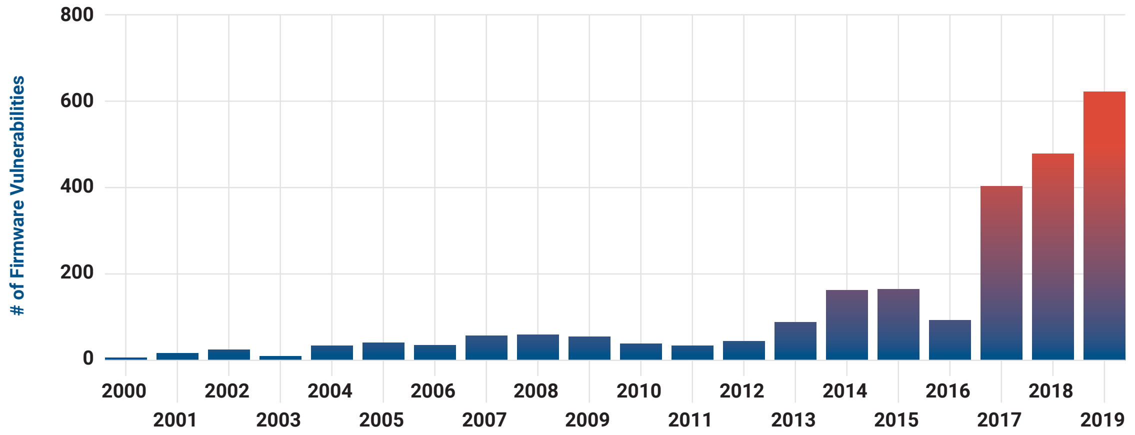
Last week Intel and Cisco published security advisories revealing dozens of vulnerabilities in firmware and hardware that impact laptops, servers and routers. Intel disclosed an incredible 77 new vulnerabilities across a broad spectrum of components, including Intel CPUs, BMC, CSME, TXT, SGX, AMT, TPM and more. There were two critical and 34 high severity bugs, some of which would allow an unauthenticated user to potentially enable escalation of privileges, information disclosure or denial of service. Two notable vulnerabilities included a timing leakage on Intel firmware-based TPM (fTPM) and an STMicroelectronics' TPM chip that allows an attacker to recover 256-bit private keys from digital signature schemes, and an updated Zombieload Attack disclosure from Graz University of Technology and KU Leuven that impacts more recent processors, including Intel's line of Cascade Lake CPUs.

Eclypsium also released an update to our research on widespread vulnerabilities in Windows drivers involving more than 40 drivers from at least 20 different vendors, adding a new disclosure about a PMX driver rated as a high severity vulnerability. Cisco added to the week's tally with multiple vulnerabilities impacting the firmware of their small business routers.

As a result, the listing of firmware vulnerabilities reported to the National Vulnerability Database in 2019 is up more than 30% from last year, and is six times larger than three years ago. For IT teams tasked with protecting infrastructure from attack, the challenge of keeping up with firmware updates has grown significantly, and the severity of the issues demonstrates how big the gaps are in firmware security.

Don't expect the rate of growth in firmware vulnerabilities to wane. At the root of this problem is the growing number and complexity of the components in laptops, servers and network devices. Dozens of components in a typical laptop now have their own firmware—often with millions of lines of code—and all are susceptible to bugs and design flaws that can impact security. Because hardware design cycles are long, updates to firmware are increasingly used to solve hardware problems, but this also introduces new attack vectors. For example, our research showed that the tool released by Intel to detect and mitigate a recent AMT vulnerability included a vulnerable driver as part of the toolset used to solve that issue. Adding to the complexity, many of the components and the associated software used in laptops, servers and network devices are part of complex third-party supply chains - for example, Cisco's security advisory referenced multiple third-party software components with firmware vulnerabilities.

Firmware Vulnerabilities By Year



Source: National Vulnerability Database November 15, 2019

Enterprise IT teams cannot afford to take these risks lightly. The FBI has warned that high-impact ransomware attacks threaten US businesses and organizations. As part of cyber defense best practices they advise patching operating system, software, and firmware. Unfortunately, many IT organizations have little visibility into which of their devices are susceptible to known vulnerabilities, such as those that emerged this week. Even worse, implanting attacker code in UEFI/BIOS or component firmware allows an attacker to achieve persistence that can survive a complete device re-imaging or disk replacement, as the MITRE ATT&CK framework spells out.

This surge of publicly disclosed vulnerabilities serves as a reminder that firmware is a part of the attack surface that every organization needs to manage both locally as well as in the cloud, to ensure that the hardware and firmware that critical organizational services rely on is secure. History has shown that publicly disclosed issues are only a fraction of the real attack surface and often serve as a catalyst; attackers will capitalize on them to not only weaponize published vulnerabilities but also leverage them to discover additional defects to compromise. Effectively managing such risk requires visibility into your attack surface to identify your exposure, an understanding of the potential ability to leverage the defects against you in spite of your existing controls, and the ability to verify when vulnerabilities are addressed and the risk is reduced to acceptable levels.