Intel Software and Firmware Updates Patch 18 High-Severity Vulnerabilities

By Eduard Kovacs on February 17, 2022

Intel has released software and firmware updates to address many vulnerabilities found in the company's products.

The chipmaker last week released 22 security advisories, including seven that have an overall severity rating of "high."

These advisories describe 18 high-severity vulnerabilities, most of which can be exploited for privilege escalation. Others can lead to information disclosure or a denial of service (DoS) condition. Exploitation of these flaws typically requires local access to the targeted device.

One advisory informs users that the BIOS firmware for some Intel processors is affected by 10 high-severity privilege escalation vulnerabilities.

Another advisory describes one serious security flaw that has been found in the Intel chipset firmware in Server Platform Services (SPS), Active Management Technology (AMT), and Power Management Controller (PMC).

High-severity issues have also been found in the Kernelflinger open source project, Intel Quartus Prime components, PROSet/Wireless WiFi and Killer WiFi products, and the AMT SDK, Setup and Configuration Software (SCS), and Management Engine BIOS eXtensions (MEBx).

The remaining advisories describe over a dozen medium- and low-severity vulnerabilities addressed by the company this month.

Some computer vendors, such as HPE, have also released advisories to inform their customers about some of the vulnerabilities affecting Intel hardware.

On one hand, considering that Intel software and firmware is widely deployed, these types of vulnerabilities could turn out to be useful to threat actors. On the other hand, CISA's Known Exploited Vulnerabilities Catalog, which includes more than 370 flaws that have been exploited in attacks over the past decade, only mentions one Intel vulnerability (CVE-2017-5689).

Intel last year patched a total of 226 vulnerabilities in its products, and it has paid out an average of $800,000 per year through its bug bounty program since its launch in 2018. Two of the flaws patched in 2021 were rated "critical" and 52 were rated "high severity."

Related: Intel CPU Vulnerability Can Expose Cryptographic Keys

Related: Intel Patches High-Severity Flaws in NUC 9 Extreme Laptops, Ethernet Linux Drivers

Related: Intel, VMware Join Patch Tuesday Parade

Eduard Kovacs (@EduardKovacs) is a contributing editor at SecurityWeek. He worked as a high school IT teacher for two years before starting a career in journalism as Softpedia's security news reporter. Eduard holds a bachelor's degree in industrial informatics and a master's degree in computer techniques applied in electrical engineering.

Previous Columns by Eduard Kovacs:
CISA Creates List of Free Cybersecurity Tools and Services for Defenders
Patch for Actively Exploited Flaw in Adobe Commerce and Magento Bypassed
VMware NSX Data Center Flaw Can Expose Virtual Systems to Attacks
Intel Software and Firmware Updates Patch 18 High-Severity Vulnerabilities
Malicious Emails Can Crash Cisco Email Security Appliances

Tags:
NEWS & INDUSTRY Vulnerabilities