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

By Eduard Kovacs on August 11, 2021

Share 发推 RSS

Intel on Tuesday released six new security advisories to inform customers about the availability of firmware and software updates that address a total of 15 vulnerabilities across several products.

Two of the advisories have been assigned a *high severity* rating. One of them describes a vulnerability affecting some Intel NUC 9 Extreme laptop kits that can be exploited by an authenticated attacker to escalate privileges. The flaw (CVE-2021-0196) is caused by improper access control issues in the kernel mode driver.

Another high-severity advisory describes three vulnerabilities affecting Intel Ethernet controller X722 and 800 series Linux drivers. The most serious of the flaws, CVE-2021-0084, can be exploited by an authenticated attacker to escalate privileges.

[**Related**: Inside Intel's Hardware-Enabled Threat Detection Push]

The other two flaws, rated *medium* and *low severity*, can lead to information disclosure and denial of service (DoS) — they both require local access for exploitation.

The remaining advisories cover medium-severity issues, including a privilege escalation bug in NUC Pro Chassis Element AverMedia Capture Card drivers, a DoS vulnerability in Optane Persistent

Memory (PMem), DoS and privilege escalation flaws in graphics drivers, and several DoS vulnerabilities in 800 series network adapters and controllers.

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) on Tuesday advised users and administrators to review the patches from Intel and take action as necessary.

Related: Intel Patches Tens of Vulnerabilities in Software, Hardware Products

Related: Intel Releases 29 Advisories to Describe 73 Vulnerabilities Affecting Its Products

Related: Intel Releases Firmware Updates to Patch Critical Vulnerability in AMT, ISM

Share 发推 RSS

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:

Decryption Key for Ransomware Delivered via Kaseya Attack Made Public
OwnBackup Raises $240 Million at $3.35 Billion Valuation
Intel Patches High-Severity Flaws in NUC 9 Extreme Laptops, Ethernet Linux Drivers
Nine Critical and High-Severity Vulnerabilities Patched in SAP Products
Firefox 91 Brings New Privacy, Security Improvements

sponsored links

Virtual Event Series - Security Summit Online Events by SecurityWeek

2021 Singapore/APAC ICS Cyber Security Conference [Virtual: June 22-24]

2021 ICS Cyber Security Conference | USA [Hybrid: Oct. 25-28]

2021 CISO Forum: September 21-22 - A Virtual Event

Tags:
NEWS & INDUSTRY Vulnerabilities

Search

Get the Daily Briefing

BRIEFING

Business Email Address Subscribe