Scottish Cyber Coordination Centre

Daily threat bulletin

25 October 2024

Vulnerabilities

Fortinet Confirms Exploitation of Critical FortiManager Zero-Day Vulnerability

Infosecurity Magazine - 24 October 2024 11:45

This high-severity flaw, dubbed FortiJump by security researcher Kevin Beaumont, has been added to CISA's KEV catalog

Cisco fixed tens of vulnerabilities, including an actively exploited one

Security Affairs - 24 October 2024 16:58

Cisco patched vulnerabilities in ASA, FMC, and FTD products, including one actively exploited in a large-scale brute-force attack campaign. Cisco addressed multiple vulnerabilities in Adaptive Security Appliance (ASA), Secure Firewall Management Center (FMC), and Firepower Threat Defense (FTD) products, including an actively exploited flaw tracked as CVE-2024-20481.

Nvidia Patches High-Severity Flaws in Windows, Linux Graphics Drivers

SecurityWeek - 24 October 2024 17:48

Nvidia rolls out urgent security updates to fix at least 8 high-severity vulnerabilities in GPU drivers for Windows and Linux.

AWS Cloud Development Kit Vulnerability Exposes Users to Potential Account Takeover Risks

The Hacker News - 24 October 2024 19:30

Cybersecurity researchers have disclosed a security flaw impacting Amazon Web Services (AWS) Cloud Development Kit (CDK) that could have resulted in an account takeover under specific circumstances.

Lazarus Group Exploits Google Chrome Flaw in New Campaign

Infosecurity Magazine - 24 October 2024 17:00

Lazarus Group exploited Google Chrome zero-day, infecting systems with Manuscrypt malware

Threat actors and malware

New Qilin.B Ransomware Variant Emerges with Improved Encryption and Evasion Tactics

The Hacker News - 24 October 2024 23:08

Cybersecurity researchers have discovered an advanced version of the Qilin ransomware sporting increased sophistication and tactics to evade detection.The new variant is being tracked by cybersecurity firm Halcyon under the moniker Qilin.B.

Samsung Galaxy S24 and Sonos Era hacked on Pwn2Own Ireland Day 2

BleepingComputer - 24 October 2024 11:01

On the second day of Pwn2Own Ireland 2024, competing white hat hackers showcased an impressive 51 zero-day vulnerabilities, earning a total of $358,625 in cash prizes. [...]

Apple creates Private Cloud Compute VM to let researchers find bugs

BleepingComputer - 24 October 2024 19:48

Apple created a Virtual Research Environment to allow public access to testing the security of its Private Cloud Compute system, and released the source code for some “key components” to help researchers analyze the privacy and safety features on the architecture. [...]

UK related

UK Government Urges Organizations to Get Cyber Essentials Certified

Infosecurity Magazine - 24 October 2024 09:00

On the 10th anniversary since Cyber Essentials was introduced, the UK government has highlighted the impact the scheme has had in preventing attacks