Scottish Cyber Coordination Centre

Daily threat bulletin

12 April 2024

Vulnerabilities

Intel and Lenovo servers impacted by 6-year-old BMC flaw

BleepingComputer - 11 April 2024 13:50

An almost 6-year-old vulnerability in the Lighttpd web server used in Baseboard Management Controllers has been overlooked by many device vendors, including Intel and Lenovo. [...]

CISA Adds Two Known Exploited Vulnerabilities to Catalog

CISA Advisories -

CISA has added two new vulnerabilities to its Known Exploited Vulnerabilities Catalog, based on evidence of active exploitation. CVE-2024-3272 D-Link Multiple NAS Devices Use of Hard-Coded Credentials Vulnerability.

Threat actors and malware

US Government on High Alert as Russian Hackers Steal Critical Correspondence From Microsoft

SecurityWeek - 11 April 2024 20:41

The US government says Midnight Blizzard's compromise of Microsoft corporate email accounts "presents a grave and unacceptable risk to federal agencies."The post US Government on High Alert as Russian Hackers Steal Critical Correspondence From Microsoft appeared first on SecurityWeek.

Apple Warns Users in 150 Countries of Mercenary Spyware Attacks

darkreading - 11 April 2024 19:19

In new threat notification information, Apple singled out Pegasus vendor NSO Group as a culprit in mercenary spyware attacks.

LastPass: Hackers targeted employee in failed deepfake CEO call

BleepingComputer - 11 April 2024 19:00

Scottish Cyber Coordination Centre

LastPass revealed this week that threat actors targeted one of its employees in a voice phishing attack, using deepfake audio to impersonate Karim Toubba, the company's Chief Executive Officer. [...]

DPRK Exploits 2 MITRE Sub-Techniques: Phantom DLL Hijacking, TCC Abuse

darkreading - 11 April 2024 21:02

North Korean hackers break ground with new exploitation techniques for Windows and macOS.

New Android Espionage Campaign Spotted in India and Pakistan

Infosecurity Magazine - 11 April 2024 15:45

A new cyber espionage campaign, called 'eXotic Visit,' targeted Android users in South Asia via seemingly legitimate messaging apps