Scottish Cyber Coordination Centre

Daily threat bulletin

25 April 2024

Vulnerabilities

Maximum severity Flowmon bug has a public exploit, patch now

BleepingComputer - 24 April 2024 17:08

Proof-of-concept exploit code has been released for a top-severity security vulnerability in Progress Flowmon, a tool for monitoring network performance and visibility. [...]

ArcaneDoor hackers exploit Cisco zero-days to breach govt networks

BleepingComputer - 24 April 2024 14:07

Cisco warned today that a state-backed hacking group has been exploiting two zero-day vulnerabilities in Adaptive Security Appliance (ASA) and Firepower Threat Defense (FTD) firewalls since November 2023 to breach government networks worldwide.

Major Security Flaws Expose Keystrokes of Over 1 Billion Chinese Keyboard App Users

The Hacker News - 24 April 2024 16:06

Security vulnerabilities uncovered in cloud-based pinyin keyboard apps could be exploited to reveal users' keystrokes to nefarious actors.The findings come from the Citizen Lab, which discovered weaknesses in eight of nine apps from vendors like Baidu, Honor, iFlytek, OPPO, Samsung, Tencent, Vivo, and Xiaomi.

Google Patches Critical Chrome Vulnerability

SecurityWeek - 24 April 2024 13:48

Google patches CVE-2024-4058, a critical Chrome vulnerability for which researchers earned a $16,000 reward. The post Google Patches Critical Chrome Vulnerability appeared first on SecurityWeek.

Threat actors and malware

Hackers hijack antivirus updates to drop GuptiMiner malware

BleepingComputer - 23 April 2024 11:56

North Korean hackers have been exploiting the updating mechanism of the eScan antivirus to plantbackdoors on big corporate networks and deliver cryptocurrency miners through GuptiMiner malware. [...]

North Korea-linked APT groups target South Korean defense contractors

Security Affairs - 23 April 2024 20:24

The National Police Agency in South Korea warns that North Korea-linked threat actors are targeting defense industry entities. The National Police Agency in South Korea warns that North Korea-linked threat actors are targeting defense industry entities to steal defense technology information.

CoralRaider Malware Campaign Exploits CDN Cache to Spread Info-Stealers

The Hacker News - 24 April 2024 11:20

A new ongoing malware campaign has been observed distributing three different stealers such as CryptBot Lumma C2, and Rhadamanthys hosted on Content Delivery Network (CDN) cache domains since at least February 2024.Cisco Talos has attributed the activity with moderate confidence to a threat actor tracked as CoralRaider.

Ransomware Gang Leaks Data Allegedly Stolen From Government Contractor

SecurityWeek - 23 April 2024 11:20

The LockBit ransomware gang leaks data allegedly stolen from government contractor Tyler Technologies. The post Ransomware Gang Leaks Data Allegedly Stolen From Government Contractor appeared first on SecurityWeek.