Scottish Cyber Coordination Centre

Daily threat bulletin

10 April 2024

Vulnerabilities

Microsoft fixes two Windows zero-days exploited in malware attacks

BleepingComputer - 09 April 2024 19:06

Microsoft has fixed two actively exploited zero-day vulnerabilities during the April 2024 Patch Tuesday, although the company failed to initially tag them as such. [...]

Critical Rust flaw enables Windows command injection attacks

BleepingComputer - 09 April 2024 17:20

Threat actors can exploit a security vulnerability in the Rust standard library to target Windows systems in command injection attacks. [...]

New SharePoint flaws help hackers evade detection when stealing files

BleepingComputer - 09 April 2024 10:00

Researchers have discovered two techniques that could enable attackers to bypass audit logs or generate less severe entries when downloading files from SharePoint. [...]

LG Smart TVs at Risk of Attacks, Thanks to 4 OS Vulnerabilities

darkreading - 09 April 2024 21:44

Scans showed that 91,000 devices are exposed and at risk for unauthorized access and TV set takeover.

SAP's April 2024 Updates Patch High-Severity Vulnerabilities

SecurityWeek - 09 April 2024 14:33

SAP has released 12 new and updated security notes on April 2024 Security Patch Day, including three notes dealing with high-severity vulnerabilities.The post SAP's April 2024 Updates Patch High-Severity Vulnerabilities appeared first on SecurityWeek.

Scottish Cyber Coordination Centre

Threat actors and malware

10-Year-Old 'RUBYCARP' Romanian Hacker Group Surfaces with Botnet

The Hacker News - 09 April 2024 20:31

A threat group of suspected Romanian origin called RUBYCARP has been observed maintaining a long-running botnet for carrying out crypto mining, distributed denial-of-service (DDoS), and phishing attacks.The group, believed to be active for at least 10 years, employs the botnet for financial gain, Sysdig said in a report shared with The Hacker News."Its primary method of operation

CVS Group Restoring Systems Impacted by Cyberattack

SecurityWeek - 09 April 2024 12:19

Veterinary services provider CVS Group is restoring systems after a cyberattack disrupted its UK operations.The post CVS Group Restoring Systems Impacted by Cyberattack appeared first on SecurityWeek.

Second Ransomware Group Extorting Change Healthcare

SecurityWeek - 09 April 2024 11:18

RansomHub is extorting Change Healthcare, threatening to release data stolen in a February 2024 BlackCat ransomware attack.The post Second Ransomware Group Extorting Change Healthcare appeared first on SecurityWeek.

Hackers Use Malware to Hunt Software Vulnerabilities

Infosecurity Magazine - 09 April 2024 17:15

Palo Alto Networks observed growing malware-initiated vulnerability scanning activity

China is using generative AI to carry out influence operations

Security Affairs - 09 April 2024 07:19

China-linked threat actors are using AI to carry out influence operations aimed at fueling social disorders in the U.S. and Taiwan. China is using generative artificial intelligence to carry out influence operations against foreign countries, including the U.S. and Taiwan, and fuel social disorders. According to the report published by the Microsoft Threat Analysis Center [...]