Scottish Cyber Coordination Centre

Daily threat bulletin

30 May 2024

Vulnerabilities

Windows 11 KB5037853 update fixes File Explorer issues, 20 bugs

BleepingComputer - 29 May 2024 19:18

Microsoft has released the May 2024 non-security preview update for Windows 11 versions 22H2 and 23H2, which includes 32 fixes and changes. [...]

Check Point releases emergency fix for VPN zero-day exploited in attacks

BleepingComputer - 29 May 2024 10:31

Check Point has released hotfixes for a VPN zero-day vulnerability exploited in attacks to gain remote access to firewalls and attempt to breach corporate networks. [...]

Vulnerabilities in Eclipse ThreadX Could Lead to Code Execution

SecurityWeek - 29 May 2024 14:51

Vulnerabilities in the real-time IoT operating system Eclipse ThreadX before version 6.4 could lead to denial-of-service and code execution.The post Vulnerabilities in Eclipse ThreadX Could Lead to Code Execution appeared first on SecurityWeek.

Threat actors and malware

Cybercriminals pose as “helpful” Stack Overflow users to push PyPI malware

BleepingComputer - 29 May 2024 20:22

Cybercriminals are abusing Stack Overflow in an interesting approach to spreading malware—answering users’ questions by promoting a malicious PyPi package that installs Windows information-stealing malware. [...]

Okta warns of credential stuffing attacks targeting its CORS feature

BleepingComputer - 29 May 2024 12:46

Okta warns that a Customer Identity Cloud (CIC) feature is being targeted in credential stuffing attacks, stating that numerous customers have been targeted since April. [...]

Microsoft Uncovers ‘Moonstone Sleet’ — New North Korean Hacker Group

The Hacker News - 29 May 2024 17:05

A never-before-seen North Korean threat actor codenamed Moonstone Sleet has been attributed as behind cyber attacks targeting individuals and organizations in the software and information technology, education, and defense industrial base sectors with ransomware

and bespoke malware previously associated with the infamous Lazarus Group."Moonstone Sleet is observed to set up fake companies and

BlackSuit Claims Dozens of Victims With Carefully Curated Ransomware

darkreading - 29 May 2024 15:43

Researchers went in-depth on an attack by the threat group, which mainly targets US companies in the education and industrial goods sectors, specifically to maximize financial gain.

New Endpoint Protection Platform by Cigent Blocks Ransomware at the Data Level

SecurityWeek - 29 May 2024 12:00

The two primary components to the solution are to encrypt company data at all times, and to decrypt only when the file is required for use.The post New Endpoint Protection Platform by Cigent Blocks Ransomware at the Data Level appeared first on SecurityWeek.