Scottish Cyber Coordination Centre

Daily threat bulletin

29 August 2024

Vulnerabilities

South Korean hackers exploited WPS Office zero-day to deploy malware

BleepingComputer - 28 August 2024 19:50

The South Korea-aligned cyberespionage group APT-C-60 has been leveraging a zero-day code execution vulnerability in the Windows version of WPS Office to install the SpyGlace backdoor on East Asian targets. [...]

U.S. CISA adds Google Chromium V8 bug to its Known Exploited Vulnerabilities catalog

Security Affairs - 28 August 2024 22:01

U.S. Cybersecurity and Infrastructure Security Agency (CISA) adds Google Chromium V8 bug to its Known Exploited Vulnerabilities catalog. The U.S. Cybersecurity and Infrastructure Security Agency (CISA) added Google Chromium V8 Inappropriate Implementation Vulnerability CVE-2024-38856 (CVSS score of 8.8) to its Known Exploited Vulnerabilities (KEV) catalog.

BlackByte Ransomware group targets recently patched VMware ESXi flaw CVE-2024-37085

Security Affairs - 28 August 2024 15:39

BlackByte ransomware operators are exploiting a recently patched VMware ESXi hypervisors vulnerability in recent attacks. Cisco Talos observed the BlackByte ransomware group exploiting the recently patched security flaw CVE-2024-37085 in VMware ESXi hypervisors in recent attacks. The flaw CVE-2024-37085 (CVSS score of 6.8) is an authentication bypass vulnerability in VMware ESXi.

Fortra Issues Patch for High-Risk FileCatalyst Workflow Security Vulnerability

The Hacker News - 28 August 2024 22:44

Fortra has addressed a critical security flaw impacting FileCatalyst Workflow that could be abused by a remote attacker to gain administrative access.The vulnerability, tracked as CVE-2024-6633, carries a CVSS score of 9.8, and stems from the use of a static password to connect to a HSQL database.

Hitachi Energy Vulnerabilities Plague SCADA Power Systems

darkreading - 28 August 2024 15:43

The company has assessed four of the five disclosed vulnerabilities as being of high to critical severity.

Scottish Cyber Coordination Centre

Threat actors and malware

New Tickler malware used to backdoor US govt, defense orgs

BleepingComputer - 28 August 2024 15:36

The APT33 Iranian hacking group has used new Tickler malware to backdoor the networks of organizations in the government, defense, satellite, oil and gas sectors in the United States and the United Arab Emirates. [...]

Iran's Pioneer Kitten hits US networks via buggy Check Point, Palo Alto gear

The Register - 28 August 2024 19:00

The government-backed crew also enjoys ransomware as a side hustle Iranian government-backed cybercriminals have been hacking into US and foreign networks as recently as this month to steal sensitive data and deploy ransomware, and they're breaking in via vulnerable VPN and firewall devices from Check Point, Citrix, Palo Alto Networks and other manufacturers, according to Uncle Sam.

LummaC2 Infostealer Resurfaces With Obfuscated PowerShell Tactics

Infosecurity Magazine - 28 August 2024 17:15

LummaC2, a C-based MaaS tool first identified in 2022, has resurfaced to exfiltrate credentials and personal data.

Cisco: BlackByte ransomware gang only posting 20% to 30% of successful attacks

The Record from Recorded Future News - 28 August 2024 21:12