Scottish Cyber Coordination Centre

Daily threat bulletin

20 May 2024

Vulnerabilities

CISA warns of hackers exploiting Chrome, EoL D-Link bugs

BleepingComputer - 19 May 2024 11:17

The U.S. Cybersecurity & Infrastructure Security Agency (CISA) has added three security vulnerabilities to its 'Known Exploited Vulnerabilities' catalog, one impacting Google Chrome and two affecting some D-Link routers. [...]

CISA adds D-Link DIR router flaws to its Known Exploited Vulnerabilities catalog

Security Affairs - 17 May 2024 11:20

CISA adds two D-Link DIR-600 and DIR-605 router vulnerabilities to its Known Exploited Vulnerabilities catalog.

CISA adds Google Chrome zero-days to its Known Exploited Vulnerabilities catalog

Security Affairs - 17 May 2024 09:50

CISA adds two Chrome zero-day vulnerabilities to its Known Exploited Vulnerabilities catalog. The U.S. Cybersecurity and Infrastructure Security Agency (CISA) added [1,2] the following vulnerabilities to its Known Exploited Vulnerabilities (KEV) catalog: CVE-2024-4761 Google Chromium V8 Engine contains an unspecified out-of-bounds memory write vulnerability via a crafted HTML page.

Intel Discloses Max Severity Bug in Its AI Model Compression Software

darkreading - 17 May 2024 20:52

The improper input validation issue in Intel Neural Compressor enables remote attackers to execute arbitrary code on affected systems.

Critical Flaw in AI Python Package Can Lead to System and Data Compromise

SecurityWeek - 17 May 2024 13:43

A critical vulnerability tracked as CVE-2024-34359 and dubbed Llama Drama can allow hackers to target AI product developers.The post Critical Flaw in AI Python Package Can Lead to System and Data Compromise appeared first on SecurityWeek.

Threat actors and malware

Ransomware gang targets Windows admins via PuTTy, WinSCP malvertising

BleepingComputer - 18 May 2024 15:23

A ransomware operation targets Windows system administrators by taking out Google ads to promote fake download sites for Putty and WinSCP. [...]

North Korea-linked Kimsuky APT attack targets victims via Messenger

Security Affairs - 17 May 2024 08:10

North Korea-linked Kimsuky APT group employs rogue Facebook accounts to target victims via Messenger and deliver malware. Researchers at Genius Security Center (GSC) identified a new attack strategy by the North Korea-linked Kimsuky APT group and collaborated with the Korea Internet & Security Agency (KISA) for analysis and response. The nation-state actor attack used a fake account [...]

Latrodectus Malware Loader Emerges as IcedID's Successor in Phishing Campaigns

The Hacker News - 20 May 2024 12:17

Cybersecurity researchers have observed a spike in email phishing campaigns starting early March 2024 that delivers Latrodectus, a nascent malware loader believed to be the successor to the IcedID malware."These campaigns typically involve a recognizable infection chain involving oversized JavaScript files that utilize WMI's ability to invoke msiexec.exe and install a remotely-hosted MSI

London Drugs cyber attack: What businesses can learn from its week-long shutdown

Security Boulevard - 18 May 2024 12:56

London Drugs cyber attack: What businesses can learn from its week-long shutdown The London Drugs cyber attack has been making headlines throughout the country. What makes this breach unique, is the impact it has had on operations and customer access. Following the attack, all 79 London Drug stores shut down for over a week.

Microsoft Quick Assist Tool Abused for Ransomware Delivery

SecurityWeek - 17 May 2024 11:47

The Black Basta group abuses remote connection tool Quick Assist in vishing attacks leading to ransomware deployment.The post Microsoft Quick Assist Tool Abused for Ransomware Delivery appeared first on SecurityWeek.

New Backdoors on a European Government's Network Appear to be Russian

Cyware News - Latest Cyber News - 18 May 2024 01:00

Researchers with the Slovak cybersecurity firm ESET published a technical analysis on Wednesday of the two backdoors by a suspected Russian threat group, which they named LunarWeb and LunarMail.