Scottish Cyber Coordination Centre

Daily Threat Bulletin

15 May 2025

Vulnerabilities

U.S. CISA adds Microsoft Windows flaws to its Known Exploited Vulnerabilities catalog

Security Affairs - 14 May 2025 21:36

U.S. Cybersecurity and Infrastructure Security Agency (CISA) adds Microsoft Windows flaws to its Known Exploited Vulnerabilities catalog. The U.S. Cybersecurity and Infrastructure Security Agency (CISA) added Microsoft Windows flaws to its Known Exploited Vulnerabilities (KEV) catalog.

New Chrome Vulnerability Enables Cross-Origin Data Leak via Loader Referrer Policy

The Hacker News - 15 May 2025 12:45

Google on Wednesday released updates to address four security issues in its Chrome web browser, including one for which it said there exists an exploit in the wild.The high-severity vulnerability, tracked as CVE-2025-4664 (CVSS score: 4.3), has been characterized as a case of insufficient policy enforcement in a component called Loader."

Samsung Patches CVE-2025-4632 Used to Deploy Mirai Botnet via MagicINFO 9 Exploit

The Hacker News - 15 May 2025 00:27

Samsung has released software updates to address a critical security flaw in MagicINFO 9 Server that has been actively exploited in the wild.The vulnerability, tracked as CVE-2025-4632 (CVSS score: 9.8), has been described as a path traversal flaw.

Vulnerabilities Patched by Juniper, VMware and Zoom

SecurityWeek - 14 May 2025 11:35

Juniper Networks, VMware, and Zoom have announced patches for dozens of vulnerabilities across their products.

ICS Patch Tuesday: Vulnerabilities Addressed by Siemens, Schneider, Phoenix Contact

SecurityWeek - 14 May 2025 08:29

Industrial giants Siemens, Schneider Electric and Phoenix Contact have released ICS security advisories on the May 2025 Patch Tuesday.

New Fortinet and Ivanti Zero Days Exploited in the Wild

Infosecurity Magazine - 14 May 2025 13:00

Scottish Cyber Coordination Centre

Fortinet and Ivanti published advisories on the same day revealing that attackers are exploiting new zero days, one of which is rated critical

CISA Adds One Known Exploited Vulnerability to Catalog

CISA Advisories -

CISA has added one new vulnerability to its Known Exploited Vulnerabilities Catalog, based on evidence of active exploitation.CVE-2025-32756 Fortinet Multiple Products Stack-Based Buffer Overflow Vulnerability.

Threat actors and malware

Hackers behind UK retail attacks now targeting US companies

BleepingComputer - 14 May 2025 16:38

Google warned today that hackers using Scattered Spider tactics against retail chains in the United Kingdom have also started targeting retailers in the United States. [...]

Steel giant Nucor Corporation facing disruptions after cyberattack

BleepingComputer - 14 May 2025 11:39

A cybersecurity incident on Nucor Corporation's systems forced the company to take offline parts of its networks and implement containment measures. [...]

BianLian and RansomExx Exploit SAP NetWeaver Flaw to Deploy PipeMagic Trojan

The Hacker News - 15 May 2025 00:20

At least two different cybercrime groups BianLian and RansomExx are said to have exploited a recently disclosed security flaw in SAP NetWeaver tracked as CVE-2025-31324, indicating that multiple threat actors are taking advantage of the bug.Cybersecurity firm ReliaQuest, in a new update published today, said it uncovered evidence suggesting involvement from the BianLian data extortion crew and

Marks & Spencer Confirms Customer Data Stolen in Cyberattack

darkreading - 14 May 2025 15:33

The British retailer said no account passwords were compromised in last month's cyberattack, but the company will require customers to reset passwords "for extra peace of mind."

Here's what we know about the DragonForce ransomware that hit Marks & Spencer

The Register - 15 May 2025 07:32

Would you believe it, this RaaS cartel says Russia is off limits DragonForce, a new-ish ransomware-as-a-service operation, has given organizations another cyber threat to worry about — unless they're in Russia, which is off limits to the would-be extortionists....

UK related

Scottish Cyber Coordination Centre

Co-op narrowly avoided an even worse cyber attack, BBC learns

BBC News - 15 May 2025 00:25

The revelation - from the criminals responsible - explains why the Co-op is getting back to business faster than M&S.