Scottish
Cyber
Coordination
Centre

Daily Threat Bulletin

16 May 2025

Vulnerabilities

Government webmail hacked via XSS bugs in global spy campaign

BleepingComputer - 15 May 2025 16:14

Hackers are running a worldwide cyberespionage campaign dubbed 'RoundPress,' leveraging zero-day and n-day flaws in webmail servers to steal email from high-value government organizations. [...]

U.S. CISA adds a Fortinet flaw to its Known Exploited Vulnerabilities catalog

Security Affairs - 15 May 2025 10:07

U.S. Cybersecurity and Infrastructure Security Agency (CISA) adds a Fortinet vulnerability to its Known Exploited Vulnerabilities catalog. The U.S. Cybersecurity and Infrastructure Security Agency (CISA) added Fortinet Multiple Products Stack-Based Buffer Overflow Vulnerability, tracked as CVE-2025-32756, 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 17:13

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.

CISA Adds Three Known Exploited Vulnerabilities to Catalog

CISA Advisories -

CISA has added three new vulnerabilities to its Known Exploited Vulnerabilities Catalog, based on evidence of active exploitation. CVE-2024-12987 DrayTek Vigor Routers OS Command Injection Vulnerability. CVE-2025-4664 Google Chromium Loader Insufficient Policy Enforcement Vulnerability. CVE-2025-42999 SAP NetWeaver Deserialization Vulnerability.

Threat actors and malware

Russia-Linked APT28 Exploited MDaemon Zero-Day to Hack Government Webmail Servers

The Hacker News - 15 May 2025 16:35

A Russia-linked threat actor has been attributed to a cyber espionage operation targeting webmail servers such as Roundcube, Horde, MDaemon, and Zimbra via cross-site scripting (XSS) vulnerabilities, including a then-zero-day in MDaemon, according to new findings from

ESET.The activity, which commenced in 2023, has been codenamed Operation RoundPress by the Slovak cybersecurity company.

Critical SAP NetWeaver Vuln Faces Barrage of Cyberattacks

darkreading - 15 May 2025 18:02

As threat actors continue to hop on the train of exploiting CVE-2025-31324, researchers are recommending that SAP administrators patch as soon as possible so that they don't fall victim next.

PowerShell-Based Loader Deploys Remcos RAT in New Fileless Attack

Infosecurity Magazine - 15 May 2025 16:00

A stealthy fileless PowerShell attack using Remcos RAT bypassed antivirus by operating in memory

UK related

Update on Marks & Spencer Cyberattack

Security Magazine - 16 May 2025 02:00

Marks & Spencer (M&S) has provided an update on the cyberattack it recently experienced.

"Endemic" Ransomware Prompts NHS to Demand Supplier Action on Cybersecurity

Infosecurity Magazine - 15 May 2025 13:30

The voluntary cybersecurity charter asks NHS suppliers to commit to eight cybersecurity pledges, amid rising attacks on healthcare