Scottish Cyber Coordination Centre

Daily Threat Bulletin

13 November 2025

Vulnerabilities

Hackers exploited Citrix, Cisco ISE flaws in zero-day attacks

BleepingComputer - 12 November 2025 10:00

An advanced threat actor exploited the critical vulnerabilities “Citrix Bleed 2” (CVE-2025-5777) in NetScaler ADC and Gateway, and CVE-2025-20337 affecting Cisco Identity Service Engine (ISE) as zero-days to deploy custom malware.

CISA Adds Three Known Exploited Vulnerabilities to Catalog

CISA Advisories -

CISA has added three new vulnerabilities to its Known Exploited Vulnerabilities (KEV) Catalog, based on evidence of active exploitation.
CVE-2025-9242 WatchGuard Firebox Out-of-Bounds Write Vulnerability
CVE-2025-12480 Gladinet Triofox Improper Access Control Vulnerability
CVE-2025-62215 Microsoft Windows Race Condition Vulnerability

Chipmaker Patch Tuesday: Over 60 Vulnerabilities Patched by Intel

SecurityWeek - 12 November 2025 11:36

Intel, AMD and Nvidia have published security advisories describing vulnerabilities found recently in their products.

Firefox 145 and Chrome 142 Patch High-Severity Flaws in Latest Releases

SecurityWeek - 13 November 2025 06:19

Google and Mozilla have released fresh Chrome and Firefox updates that address multiple high-severity security defects.

High-Severity Vulnerabilities Patched by Ivanti and Zoom

SecurityWeek - 12 November 2025 13:07

Ivanti and Zoom resolved security defects that could lead to arbitrary file writes, elevation of privilege, code execution, and information disclosure.

Synology patches critical BeeStation RCE flaw shown at Pwn2Own Ireland 2025

Security Affairs - 12 November 2025 11:02

Synology fixed a critical BeeStation RCE flaw (CVE-2025-12686) shown at Pwn2Own, caused by unchecked buffer input allowing code execution.

Scottish Cyber Coordination Centre

ICS Patch Tuesday: Vulnerabilities Addressed by Siemens, Rockwell, Aveva, Schneider

SecurityWeek - 12 November 2025 09:06

An Aveva vulnerability also impacts Schneider Electric products and both vendors have published advisories.

Threat actors and malware

DanaBot malware is back to infecting Windows after 6-month break

BleepingComputer - 12 November 2025 12:34

The DanaBot malware has returned with a new version observed in attacks, six-months after law enforcement's Operation Endgame disrupted its activity in May.

Over 67,000 Fake npm Packages Flood Registry in Worm-Like Spam Attack

The Hacker News - 13 November 2025 11:28

Cybersecurity researchers are calling attention to a large-scale spam campaign that has flooded the npm registry with thousands of fake packages since early 2024 as part of a likely financially motivated effort.

Google Sues Chinese Cybercriminals Behind 'Lighthouse' Phishing Kit

SecurityWeek - 12 November 2025 13:59

Google is targeting the threat group known as Smishing Triad, which used over 194,000 malicious domains in a campaign.

UK incidents

UK's Cyber Security and Resilience Bill makes Parliamentary debut

The Register - 12 November 2025 11:54

Various touch-ups added as MPs seek greater resilience to attacks on critical sectors. The UK government introduced the Cyber Security and Resilience (CSR) Bill to Parliament today, marking a significant overhaul of local cybersecurity legislation to sharpen the security posture of the most critical sectors.