Scottish Cyber Coordination Centre

Daily Threat Bulletin

10 November 2025

Vulnerabilities

Cisco: Actively exploited firewall flaws now abused for DoS attacks

BleepingComputer - 07 November 2025 11:44

Cisco warned this week that two vulnerabilities, which have been exploited in zero-day attacks, are now being abused to force ASA and FTD firewalls into reboot loops.

Dangerous runC flaws could allow hackers to escape Docker containers

BleepingComputer - 09 November 2025 11:11

Three newly disclosed vulnerabilities in the runC container runtime used in Docker and Kubernetes could be exploited to bypass isolation restrictions and get access to the host system.

QNAP fixed multiple zero-days in its software demonstrated at Pwn2Own 2025

Security Affairs - 10 November 2025 01:01

QNAP patched seven zero-day vulnerabilities exploited at Pwn2Own Ireland 2025. The flaws affected QTS, QuTS hero, Hyper Data Protector, Malware Remover, and HBS 3 Hybrid Backup Sync.

Chrome 142 Update Patches High-Severity Flaws

SecurityWeek - 07 November 2025 11:35

An out-of-bounds write flaw in WebGPU tracked as CVE-2025-12725 could be exploited for remote code execution.

Threat actors and malware

Landfall Android Spyware Targeted Samsung Phones via Zero-Day

SecurityWeek - 07 November 2025 16:29

Threat actors exploited CVE-2025-21042 to deliver malware via specially crafted images to users in the Middle East.

ClickFix Attacks Against macOS Users Evolving

SecurityWeek - 07 November 2025 14:22

ClickFix prompts typically contain instructions for Windows users, but now they are tailored for macOS and they are getting increasingly convincing.

Scottish Cyber Coordination Centre

GlassWorm malware returns on OpenVSX with 3 new VSCode extensions

BleepingComputer - 08 November 2025 12:17

The GlassWorm malware campaign, which impacted the OpenVSX and Visual Studio Code marketplaces last month, has returned with three new VSCode extensions that have already been downloaded over 10,000 times.

Microsoft Uncovers 'Whisper Leak' Attack That Identifies AI Chat Topics in Encrypted Traffic

The Hacker News - 08 November 2025 20:59

Microsoft has disclosed details of a novel side-channel attack targeting remote language models that could enable a passive adversary with capabilities to observe network traffic to glean details about model conversation topics despite encryption protections under certain circumstances.

Russian Hacking Group Sandworm Deploys New Wiper Malware in Ukraine

Infosecurity Magazine - 07 November 2025 13:20

Sandworm deployed data wipers against Ukrainian governmental entities and companies in the energy, logistics and grain sectors.

Data breach at Chinese infosec firm reveals cyber-weapons and target list

The Register - 10 November 2025 00:51

Chinese infosec blog MXRN last week reported a data breach at a security company called Knownsec that has ties to Beijing and Chinas military.

UK incidents

Bank of England says JLR's cyberattack contributed to UK's unexpectedly slower GDP growth

The Register - 07 November 2025 12:44

The Bank of England (BoE) has cited the cyberattack on Jaguar Land Rover (JLR) as one of the reasons for the country's slower-than-expected GDP growth in its latest rates decision.