



Scottish
Cyber
Coordination
Centre

Daily Threat Bulletin

15 September 2026

Vulnerabilities

[Hackers Exploit Critical Cisco Secure Email Gateway Vulnerability in the Wild to Run Malicious Code](#)

Cyber Security News - 15 September 2026 05:14

Cisco has issued an urgent warning regarding an actively exploited zero-day vulnerability in its Secure Email Gateway appliances that allows remote, unauthenticated attackers to execute arbitrary commands with highest-level root privileges.

[Hackers Exploit FortiGate SSL-VPN Vulnerability to Attack Broadband Provider](#)

Cyber Security News - 14 September 2026 18:08

Researchers have uncovered an exposed attacker-controlled staging server containing evidence of a wide-ranging intrusion targeting 3BB, the consumer brand operated by Thailand's Triple T Broadband.

[Telegram Desktop Flaw Lets Hidden JavaScript Exfiltrate Messages From HTML Exports](#)

The Hacker News - 15 September 2026 00:28

A flaw in Telegram Desktop let a bot's message plant hidden JavaScript inside chats that users exported to HTML files, security researchers at ExPatch said in a writeup published on September 12.

[Maximum Severity GitLab Flaw Puts Supply Chains at Risk](#)

darkreading - 14 September 2026 21:19

CVE-2026-85706 is a path traversal vulnerability with a 10 out of 10 CVSS score, affecting both GitLab Community Edition and Enterprise Edition instances.

[CISA Adds One Known Exploited Vulnerability to Catalog](#)

CISA Advisories -

CISA has added one new vulnerability to its Known Exploited Vulnerabilities (KEV) Catalog, based on evidence of active exploitation. CVE-2026-76461 Cisco Secure Email Gateway SQL Injection Vulnerability This type of vulnerability is a frequent attack vector for malicious cyber actors and poses significant risks to the federal enterprise.

Threat actors and malware

[Hackers Hijack HBO Max Reddit Account to Push 108 ClickFix Malware Ads](#)

Cyber Security News - 15 September 2026 07:56

Hackers have used a trusted Reddit identity to turn advertisements into a malware delivery channel. A compromised, verified HBO Max account, u/hbomax, published 108 malicious ClickFix ads over 48 hours, sending people toward fake software pages.

ENISA: Frontier AI Is Changing the Speed of Cyberattacks. Europe Needs to Catch Up

Security Affairs - 14 September 2026 21:35

Frontier AI is compressing the attack lifecycle from vulnerability discovery to exploitation, forcing defenders to detect, patch and respond at machine speed. Cybersecurity has always been a race between attackers and defenders. ENISA's latest assessment suggests that frontier AI is changing the speed of that race, and the gap between discovering a vulnerability and exploiting [...]

China-Linked Hackers Exploit Chrome-Windows Zero-Day Chain to Deploy GRIMWEDGE

The Hacker News - 15 September 2026 12:01

A Chinese threat actor has been attributed to a spear-phishing campaign that exploits recently patched security flaws in Google Chrome and Microsoft Windows to deliver a malicious JavaScript backdoor called GRIMWEDGE.

UK related

UK.gov begins killing off passwords for 23 million users

The Register - 14 September 2026 12:16

Passkeys promise fewer phishing headaches – and £600 a day off Whitehall's SMS bill

We must heed warnings of AI tech developers, says UK minister

BBC News - 15 September 2026 06:00

Louise Haigh is set to address growing concerns over AI safety on Tuesday in comments at the TUC Congress.