



Scottish
Cyber
Coordination
Centre

Daily Threat Bulletin

30 May 2025

Vulnerabilities

[The OWASP Top 10 Vulnerabilities](#)

Security Boulevard - 29 May 2025 21:11

Stay updated on the latest in web application security with the Open Worldwide Application Security Project (OWASP) Top 10 vulnerabilities.

[Chinese Hacking Group 'Earth Lamia' Targets Multiple Industries](#)

SecurityWeek - 29 May 2025 17:09

The highly active threat actor Earth Lamia has been observed exploiting known security defects in various public-facing assets, but mainly targeting SQL injection vulnerabilities in web applications.

Threat actors and malware

[Threat actors abuse Google Apps Script in evasive phishing attacks](#)

BleepingComputer - 29 May 2025 13:25

Threat actors are abusing the trusted Google platform 'Google Apps Script' to host phishing pages, making them appear legitimate and eliminating the risk of them getting flagged by security tools.

[Apple Safari exposes users to fullscreen browser-in-the-middle attacks](#)

BleepingComputer - 29 May 2025 13:06

A weakness in Apple's Safari web browser allows threat actors to leverage the fullscreen browser-in-the-middle (BitM) technique to steal account credentials from unsuspecting users.

[China-linked APT41 used Google Calendar as C2 to control its TOUGHPROGRESS malware](#)

Security Affairs - 29 May 2025 12:17

Google warns that China-linked APT41 used TOUGHPROGRESS malware with Google Calendar as C2, targeting various government entities via a compromised website.



Scottish
Cyber
Coordination
Centre

Malware Analysis Reveals Sophisticated RAT With Corrupted Headers

Infosecurity Magazine - 29 May 2025 14:00

Fortinet has identified a new Windows RAT operating stealthily on compromised systems with advanced evasion techniques

ConnectWise says nation-state attack targeted multiple ScreenConnect customers

The Record from Recorded Future News - 29 May 2025 20:06

IT management software company ConnectWise said it is investigating a nation-state attack on its systems that impacted some of its customers.

Victoria's Secret Website Taken Offline After Cyberattack

SecurityWeek - 29 May 2025 12:30

Lingerie retailer Victoria's Secret has fallen victim to a cyberattack that forced it to take its website down on Wednesday. The site remains offline at the time of publication.