Scottish Cyber Coordination Centre

Daily Threat Bulletin

10 March 2026

Vulnerabilities

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-2021-22054 Omnissa Workspace ONE Server-Side Request Forgery

CVE-2025-26399 SolarWinds Web Help Desk Deserialization of Untrusted Data Vulnerability

CVE-2026-1603 Ivanti Endpoint Manager (EPM) Authentication Bypass Vulnerability

Threat Actor Exploits Flaws and Uses Elastic Cloud SIEM to Manage Stolen Data

Infosecurity Magazine - 09 March 2026 16:45

Huntress researchers uncover campaign exploiting vulnerabilities to steal data using Elastic Cloud as a data hub.

Google: Cloud attacks exploit flaws more than weak credentials

BleepingComputer - 09 March 2026 18:45

Hackers are increasingly exploiting newly disclosed vulnerabilities in third-party software to gain initial access to cloud environments, with the window for attacks shrinking from weeks to just days.

Anthropic Claude Opus AI model discovers 22 Firefox bugs

Security Affairs - 09 March 2026 08:10

Anthropic discovered 22 security vulnerabilities in Firefox using its Claude Opus 4.6 AI model in January 2026. Mozilla addressed these issues in Firefox 148.

Threat actors and malware

Microsoft Teams phishing targets employees with A0Backdoor malware

BleepingComputer - 09 March 2026 19:50

Hackers contacted employees at financial and healthcare organizations over Microsoft Teams to trick them into granting remote access through Quick Assist and deploy a new piece of malware called A0Backdoor.

Scottish Cyber Coordination Centre

ClickFix Attack Uses Windows Terminal to Evade Detection

SecurityWeek - 09 March 2026 13:51

Fake CAPTCHA pages instruct victims to paste malicious commands in the Windows Terminal instead of the Run dialog.

Russia-linked hackers target Signal, WhatsApp of officials globally

Security Affairs - 09 March 2026 15:54

Dutch intelligence agencies (MIVD and AIVD) warn of a global campaign by Russia-linked threat actors aiming to compromise Signal and WhatsApp accounts. The operation targets government officials, civil servants, and military personnel, highlighting growing cyber risks to sensitive communications among national security actors.

ShinyHunters claims ongoing Salesforce Aura data theft attacks

BleepingComputer - 09 March 2026 14:12

Salesforce is warning customers that hackers are targeting websites with misconfigured Experience Cloud platforms that give guest users access to more data than intended. However, the ShinyHunters extortion gang claims to be actively exploiting a new bug to steal data from instances.

UK incidents

UK Launches New Crackdown Unit to Tackle Cyber-Fraud at the Source

Infosecurity Magazine - 09 March 2026 15:00

New UK Online Crime Centre will combine expertise from a range of sources to takedown online channels cyber-scammers rely on.