Scottish Cyber Coordination Centre

Daily Threat Bulletin

26 January 2026

Vulnerabilities

CISA confirms active exploitation of four enterprise software bugs

BleepingComputer - 23 January 2026 14:47

The Cybersecurity and Infrastructure Security Agency (CISA) in the U.S. warned of active exploitation of four vulnerabilities impacting enterprise software from Versa and Zimbra, the Vite frontend tooling framework, and the Prettier code formatter. [...]

Hackers exploit critical telnetd auth bypass flaw to get root

BleepingComputer - 23 January 2026 12:21

A coordinated campaign has been observed targeting a recently disclosed critical-severity vulnerability that has been present in the GNU InetUtils telnetd server for 11 years. [...]

CISA Adds Actively Exploited VMware vCenter Flaw CVE-2024-37079 to KEV Catalog

The Hacker News - 24 January 2026 14:39

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) on Friday added a critical security flaw affecting Broadcom VMware vCenter Server that was patched in June 2024 to its Known Exploited Vulnerabilities (KEV) catalog, citing evidence of active exploitation in the wild.

Exploited Zero-Day Flaw in Cisco UC Could Affect Millions

darkreading - 23 January 2026 21:56

Mass scanning is underway for CVE-2026-20045, which Cisco tagged as critical because successful exploitation could lead to a complete system takeover.

Europe's GCVE Raises Concerns Over Fragmentation in Vulnerability Databases

darkreading - 23 January 2026 21:31

GCVE would enhance global collaboration, flexibility, and efficiency in tracking security flaws. Duplicate entries and a decentralization policy may create more chaos for defenders.

Fortinet admits FortiGate SSO bug still exploitable despite December patch

The Register - 23 January 2026 13:43

Fix didn't quite do the job – attackers spotted logging in Fortinet has confirmed that attackers are actively bypassing a December patch for a critical FortiCloud single sign-on (SSO) authentication flaw after customers reported suspicious logins on devices supposedly fully up to date....

Fresh SmarterMail Flaw Exploited for Admin Access

SecurityWeek - 23 January 2026 11:34

The exploitation of the authentication bypass vulnerability started two days after patches were released.

AIs are Getting Better at Finding and Exploiting Internet Vulnerabilities

Schneier on Security - 23 January 2026 13:01

Really interesting blog post from Anthropic:In a recent evaluation of AI models' cyber capabilities, current Claude models can now succeed at multistage attacks on networks with dozens of hosts using only standard, open-source tools, instead of the custom tools needed by previous generations.

Threat actors and malware

Konni hackers target blockchain engineers with AI-built malware

BleepingComputer - 24 January 2026 11:23

The North Korean hacker group Konni (Opal Sleet, TA406) is using AI-generated PowerShell malware to target developers and engineers in the blockchain sector. [...]

ShinyHunters claim hacks of Okta, Microsoft SSO accounts for data theft

BleepingComputer - 23 January 2026 19:35

The ShinyHunters extortion gang claims it is behind a wave of ongoing voice phishing attacks targeting single sign-on (SSO) accounts at Okta, Microsoft, and Google, enabling threat actors to breach corporate SaaS platforms and steal company data for extortion. [...]

Hackers exploit critical telnetd auth bypass flaw to get root

BleepingComputer - 23 January 2026 12:21

A coordinated campaign has been observed targeting a recently disclosed critical-severity vulnerability that has been present in the GNU InetUtils telnetd server for 11 years. [...]

Osiris ransomware emerges, leveraging BYOVD technique to kill security tools

Security Affairs - 24 January 2026 19:17

Researchers identified a new Osiris ransomware used in a November 2025 attack, abusing the POORTRY driver via BYOVD to disable security tools. Symantec and Carbon Black researchers uncovered a new ransomware strain named Osiris.

Phishing Attack Uses Stolen Credentials to Install LogMeIn RMM for Persistent Access

The Hacker News - 23 January 2026 17:48

Cybersecurity researchers have disclosed details of a new dual-vector campaign that leverages stolen credentials to deploy legitimate Remote Monitoring and Management (RMM) software for persistent remote access to compromised hosts."Instead of deploying

custom viruses, attackers are bypassing security perimeters by weaponizing the necessary IT tools that administrators trust."

Microsoft Flags Multi-Stage AitM Phishing and BEC Attacks Targeting Energy Firms

The Hacker News - 23 January 2026 14:55

Microsoft has warned of a multi-stage adversary-in-the-middle (AitM) phishing and business email compromise (BEC) campaign targeting multiple organizations in the energy sector.

AI-powered cyberattack kits are 'just a matter of time,' warns Google exec

The Register - 23 January 2026 18:10

Security chief says criminals are already automating workflows, with full end-to-end tools likely within years CISOs must prepare for "a really different world" where cybercriminals can reliably automate cyberattacks at scale, according to a senior Googler....

UK related

London boroughs limping back online months after cyberattack

The Register - 23 January 2026 11:34

Direct debits? Maybe February. Birth certificates? Dream on. Council tax bills? Oh, those are coming Hammersmith & Fulham Council says payments are now being processed as usual, two months after a cyberattack that affected multiple boroughs in the UK's capital city....

NHS Issues Open Letter Demanding Improved Cybersecurity Standards from Suppliers

Infosecurity Magazine - 23 January 2026 15:38

Open letter by NHS technology leaders outlines plans to identify risks to software supply chain security across health and social care system