Scottish Cyber Coordination Centre

# Daily Threat Bulletin

27 January 2026

## Vulnerabilities

### Microsoft patches actively exploited Office zero-day vulnerability

BleepingComputer - 26 January 2026 14:20

Microsoft has released emergency security updates to patch a high-severity Office zero-day vulnerability exploited in attacks. [...]

### Dormakaba flaws allow to access major organizations' doors

Security Affairs - 27 January 2026 07:14

Researchers found over 20 flaws in Dormakaba access systems that could let attackers remotely unlock doors at major organizations. Researchers from SEC Consult discovered and fixed more than 20 security flaws in Dormakaba physical access control systems.

### Emergency Microsoft update fixes in-the-wild Office zero-day

Security Affairs - 26 January 2026 20:03

Microsoft issued emergency updates to fix an actively exploited Office zero-day, CVE-2026-21509, affecting Office 2016–2024 and Microsoft 365 Apps. Microsoft released out-of-band security updates to address an actively exploited Office zero-day vulnerability tracked as CVE-2026-21509.

### Critical CERT-In Advisories – January 2026: SAP, Microsoft, and Atlassian Vulnerabilities

Security Boulevard - 27 January 2026 07:47

January 2026 was a wake-up month for enterprise security teams. In a single week, CERT-In released three high-severity advisories exposing critical flaws across SAP, Microsoft, and Atlassian, the very platforms that run finance systems, identity layers, developer pipelines, and collaboration tools inside most enterprises.

### CISA Adds Five Known Exploited Vulnerabilities to Catalog

CISA Advisories -

CISA has added five new vulnerabilities to its Known Exploited Vulnerabilities (KEV) Catalog, based on evidence of active exploitation: CVE-2018-14634 Linux Kernel Integer Overflow Vulnerability; CVE-2025-52691 SmarterTools SmarterMail Unrestricted Upload of File with Dangerous Type Vulnerability; CVE-2026-21509 Microsoft Office Security Feature Bypass Vulnerability; CVE-2026-23760 SmarterTools SmarterMail Authentication Bypass Using an Alternate Path or Channel Vulnerability; CVE-2026-24061 GNU InetUtils Argument Injection Vulnerability.

Scottish Cyber Coordination Centre

# Threat actors and malware

## New ClickFix attacks abuse Windows App-V scripts to push malware

BleepingComputer - 26 January 2026 17:42

A new malicious campaign mixes the ClickFix method with fake CAPTCHA and a signed Microsoft Application Virtualization (App-V) script to ultimately deliver the Amatera infostealing malware. [...]

## Nearly 800,000 Telnet servers exposed to remote attacks

BleepingComputer - 26 January 2026 11:19

Internet security watchdog Shadowserver tracks nearly 800,000 IP addresses with Telnet fingerprints amid ongoing attacks exploiting a critical authentication bypass vulnerability in the GNU InetUtils telnetd server. [...]

## Hackers can bypass npm's Shai-Hulud defenses via Git dependencies

BleepingComputer - 26 January 2026 10:02

The defense mechanisms that NPM introduced after the 'Shai-Hulud' supply-chain attacks have weaknesses that allow threat actors to bypass them via Git dependencies. [...]

## Energy sector targeted in multi-stage phishing and BEC campaign using SharePoint

Security Affairs - 26 January 2026 13:38

Microsoft warns of a multi-stage phishing and BEC campaign hitting energy firms, abusing SharePoint links and inbox rules to steal credentials. Microsoft reports an active multi-stage phishing campaign targeting energy sector organizations. The campaign misused SharePoint file-sharing to deliver phishing links and created inbox rules to hide malicious activity and maintain persistence.

## North Korea–linked KONNI uses AI to build stealthy malware tooling

Security Affairs - 26 January 2026 11:47

Check Point links an active phishing campaign to North Korea–aligned KONNI, targeting developers with fake blockchain project docs and using an AI-written PowerShell backdoor. Check Point Research uncovered an active phishing campaign attributed to the North Korea–linked KONNI group (aka Kimsuky, Earth Imp, TA406, Thallium, Vedalia, and Velvet Chollima).

## 'Stanley' Malware Toolkit Enables Phishing via Website Spoofing

SecurityWeek - 26 January 2026 12:44

Priced $2,000 - $6,000 on a cybercrime forum, the MaaS toolkit promises publication on the Chrome Web Store.

## Okta Flags Customized, Reactive Vishing Attacks Which Bypass MFA

Infosecurity Magazine - 26 January 2026 13:12

Scottish Cyber Coordination Centre

Threat actors posing as IT support teams use phishing kits to generate fake login sites in real-time to trick victims into handing over credentials