Scottish Cyber Coordination Centre

Daily Threat Bulletin

11 February 2026

Vulnerabilities

Microsoft Patch Tuesday security updates for February 2026 fix six actively exploited zero-days

Security Affairs - 10 February 2026 23:31

Microsoft Patch Tuesday security updates for February 2026 fix 58 new security flaws across Windows, Office, Azure, Edge, Exchange, Hyper-V, WSL, and other components, rising to 62 CVEs when third-party updates are included.

CISA Adds Six Known Exploited Vulnerabilities to Catalog

CISA Advisories -

CISA has added six new vulnerabilities to its Known Exploited Vulnerabilities (KEV) Catalog, based on evidence of active exploitation.

CVE-2026-21510 Microsoft Windows Shell Protection Mechanism Failure Vulnerability

CVE-2026-21513 Microsoft MSHTML Framework Security Feature Bypass Vulnerability

CVE-2026-21514 Microsoft Office Word Reliance on Untrusted Inputs in a Security Decision Vulnerability

CVE-2026-21519 Microsoft Windows Type Confusion Vulnerability

CVE-2026-21525 Microsoft Windows NULL Pointer Dereference Vulnerability

CVE-2026-21533 Windows Remote Desktop Services Elevation of Privilege Vulnerability

Fortinet Patches Critical SQLi Flaw Enabling Unauthenticated Code Execution

The Hacker News - 10 February 2026 20:00

Fortinet has released security updates to address a critical flaw impacting FortiClientEMS that could lead to the execution of arbitrary code on susceptible systems. The vulnerability, tracked as CVE-2026-21643, has a CVSS rating of 9.1 out of a maximum of 10.0.

Patch Tuesday: Adobe Fixes 44 Vulnerabilities in Creative Apps

SecurityWeek - 10 February 2026 18:36

The company has fixed several critical vulnerabilities that can be exploited for arbitrary code execution.

SAP Patches Critical CRM, S/4HANA, NetWeaver Vulnerabilities

SecurityWeek - 10 February 2026 15:54

SAP has released 26 new and one updated security notes on February 2026 security patch day.

Scottish Cyber Coordination Centre

Threat actors and malware

ZeroDayRAT malware grants full access to Android, iOS devices

BleepingComputer - 10 February 2026 09:00

A new commercial mobile spyware platform dubbed ZeroDayRAT is being advertised to cybercriminals on Telegram as a tool that provides full remote control over compromised Android and iOS devices.

Warlock Ransomware Breaches SmarterTools Through Unpatched SmarterMail Server

The Hacker News - 10 February 2026 16:54

SmarterTools confirmed last week that the Warlock (aka Storm-2603) ransomware gang breached its network by exploiting an unpatched SmarterMail instance. The incident took place on January 29, 2026, when a mail server that was not updated to the latest version was compromised.

European Governments Breached in Zero-Day Attacks Targeting Ivanti

Infosecurity Magazine - 10 February 2026 10:45

The European Commission and government agencies in Finland and the Netherlands have suffered potentially related breaches.

NCSC Issues Warning Over “Severe” Cyber-Attacks Targeting Critical National Infrastructure

Infosecurity Magazine - 10 February 2026 12:50

NCSC call firms to ‘act now’ following disruptive malware attacks targeting Polish energy providers.