Scottish Cyber Coordination Centre

Daily Threat Bulletin

12 August 2026

Vulnerabilities

CISA: Microsoft SharePoint flaw now exploited in ransomware attacks

BleepingComputer - 11 August 2026 09:12

CISA confirmed today that ransomware gangs have begun abusing a high-severity Microsoft SharePoint remote code execution vulnerability, which has been flagged as actively exploited since early July.

Cisco Warns of Seven ClamAV Flaws, Two With Public PoCs

Security Affairs - 11 August 2026 17:05

Cisco warned that seven ClamAV vulnerabilities affect its Secure Endpoint Connector on Windows, macOS and Linux. ClamAV is an open-source antivirus engine widely used to scan files and emails for malware.

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-2026-20349 Cisco Secure Firewall Adaptive Security Appliance (ASA) and Firewall Threat Defense (FTD) Heap Inspection Vulnerability

CVE-2026-68820 Microsoft Windows Ancillary Function Driver for WinSock Use-After-Free Vulnerability

CVE-2026-72898 Metabase SQL Injection Vulnerability

Microsoft August 2026 Patch Tuesday fixes 400 flaws, 3 zero-days

BleepingComputer - 11 August 2026 15:08

Today is Microsoft's August 2026 Patch Tuesday, and with it comes security updates for a massive 400 flaws, including one actively exploited and two publicly disclosed zero-day vulnerabilities.

Adobe Urges Immediate Patching of Critical ColdFusion, Campaign Classic Flaws

SecurityWeek - 11 August 2026 17:50

The security defects could be exploited for arbitrary code execution and denial-of-service.

Scottish Cyber Coordination Centre

Zoom Annotation Flaws Could Let a Meeting Participant Hijack Another Attendee's Client

The Hacker News - 12 August 2026 01:38

Anyone sharing their screen on a Zoom call could have taken over the computers of everyone watching, and anyone watching could have taken over the presenter's. The flaw sat in the annotation tool, the feature that lets participants draw and type on a shared screen, and it asked nothing of the victim beyond being in the meeting.

SAP Patches Critical Code Injection, Memory Corruption Vulnerabilities

SecurityWeek - 11 August 2026 15:14

SAP released 28 new and two updated security notes, including four notes dealing with critical-severity bugs.

Threat actors and malware

DeadLock ransomware uses blockchain to resist infrastructure takedown

BleepingComputer - 11 August 2026 19:15

The DeadLock ransomware operation is using a decentralized infrastructure that relies on blockchain-backed services to protect its communication with victims and data-leak activity.

Gunra Ransomware Exploits Fortinet and Schneider Electric Flaws to Breach Networks

The Hacker News - 11 August 2026 15:46

Cybersecurity and intelligence agencies from South Korea and the U.S. warned of Gunra ransomware attacks targeting critical infrastructure sectors and organizations across the world.