Scottish Cyber Coordination Centre

Daily Threat Bulletin

31/08/2026

Vulnerabilities

CISA Vulnerability Review

CISA Advisories -

Most compromises do not rely on advanced techniques or cutting-edge tools. Cyber threat actors scan the internet looking for exposed, well-known software vulnerabilities to exploit. Basic security failures enable most compromises and organizations can reduce their risk by addressing these underlying weaknesses and prioritizing vulnerabilities for action based on the risk they pose.

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-2015-3246 Red Hat Libuser Race Condition Vulnerability
CVE-2015-5287 Red Hat Automatic Bug Reporting Tool Privilege Escalation
CVE-2019-1068 Microsoft SQL Server Remote Code Execution Vulnerability
CVE-2021-23758 Ajax.NET Professional Deserialization of Untrusted Data Vulnerability
CVE-2022-0995 Linux Kernel Out-of-Bounds Write Vulnerability
CVE-2026-8452 Citrix NetScaler ADC and NetScaler Gateway Improper Restriction of Operations within the Bounds of a Memory Buffer Vulnerability

CISA Adds One Known Exploited Vulnerability to Catalog

CISA Advisories -

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

CVE-2026-21962 Oracle HTTP Server and Oracle Weblogic Server Proxy Plug-in Improper Access Control Vulnerability.

CISA Adds Four Known Exploited Vulnerabilities to Catalog

CISA Advisories -

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

CVE-2026-33824 Microsoft Internet Key Exchange (IKE) Service Extensions Double Free Vulnerability

Scottish Cyber Coordination Centre

CVE-2026-55040 Microsoft SharePoint Weak Authentication Vulnerability
CVE-2026-59310 Broadcom VMware vCenter Path Traversal Vulnerability
CVE-2026-65400 Apple macOS Improper Authentication Vulnerability

Threat actors and malware

Anthropic warns infostealer malware is hijacking Claude sessions to drain usage

BleepingComputer - 30 August 2026 11:30

Anthropic is warning some Claude users that infostealer malware on their PCs has stolen active Claude login sessions, allowing attackers to access accounts and consume their usage.

Hackers Are Probing PaperCut Servers, and 47% Still Have No Patch

Security Affairs - 30 August 2026 12:26

PaperCut servers are under active attack, while 47% of tracked installations still run unpatched versions vulnerable to remote code execution. PaperCut, the print management software running in schools, hospitals, and offices worldwide, confirmed on August 27 that a pre-authentication remote code execution flaw is being actively exploited against real customers.

Defending Against an Active Threat to Siemens S7 Series PLCs

CISA Advisories -

This advisory relates to an active threat to Siemens S7 Series programmable logic controllers (PLCs). However, ongoing PLC targeting activity is broader than Siemens PLCs. All PLC owners and operators should apply relevant mitigations to reduce the risk to their devices and systems.

UK related

FulcrumSec claims Manchester Airports hack, theft of 86 GB of data

BleepingComputer - 30 August 2026 12:00

FulcrumSec claims it stole 86 GB of data from Manchester Airports Group.