Scottish Cyber Coordination Centre

Daily Threat Bulletin

15 July 2026

Vulnerabilities

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-2026-15409 SonicWall SMA1000 Appliances Server-Side Request Forgery Vulnerability

CVE-2026-15410 SonicWall SMA1000 Appliances Code Injection Vulnerability

CVE-2026-56155 Microsoft Active Directory Federation Services Insufficient Granularity of Access Control Vulnerability

CVE-2026-56164 Microsoft SharePoint Server Missing Authentication for Critical Function Vulnerability

SonicWall warns of SMA1000 flaws exploited in zero-day attacks, patch now

BleepingComputer - 14 July 2026 18:23

SonicWall warns that threat actors have been exploiting two SMA1000 vulnerabilities, tracked as CVE-2026-15409 and CVE-2026-15410, in zero-day attacks and urges customers to install the newly released security updates.

Microsoft July 2026 Patch Tuesday fixes massive 570 flaws, 3 zero-days

BleepingComputer - 14 July 2026 15:01

Today is Microsoft's July 2026 Patch Tuesday, and with it comes security updates for a record-breaking 570 flaws, including two zero-day vulnerabilities exploited in attacks and one publicly disclosed.

SAP Patches CVSS 9.9 NetWeaver ABAP Flaw That Could Expose or Modify Data

The Hacker News - 15 July 2026 00:47

SAP has rolled out updates to address multiple vulnerabilities as part of its July 2026 security updates, including a critical flaw in SAP NetWeaver Application Server ABAP.

Adobe Patches Critical ColdFusion Vulnerabilities

SecurityWeek - 14 July 2026 18:06

The ColdFusion security defects could allow attackers to execute arbitrary code or elevate their privileges.

Scottish Cyber Coordination Centre

7 Severe Vulnerabilities Patched in VMware Avi Load Balancer

SecurityWeek - 14 July 2026 14:55

The flaws can be exploited for authentication bypass, remote code execution, privilege escalation, and directory traversal.

Researchers Say Claude for Chrome Flaw Lets Rogue Extensions Trigger Gmail Reads

The Hacker News - 14 July 2026 23:57

Any other browser extension that can run a script on claude.ai can still trigger Claude for Chrome tasks aimed at your Gmail, your latest Google Doc and its comments, and your Calendar.

New MacOS Malware Exploits Legitimate Developer ID to Pose as Apple Crash Reporter

Infosecurity Magazine - 14 July 2026 13:00

Researchers at Jamf Threat Labs detail CrashStealer, which steals passwords, cryptocurrency wallets and more.

Threat actors and malware

Nearly 300 GitHub repos pose as legit software to push malware

BleepingComputer - 14 July 2026 16:15

A threat actor has published hundreds of fake GitHub repositories impersonating legitimate software and security projects to distribute infostealer malware.

New phishing kits target Microsoft 365 accounts, evade MFA

BleepingComputer - 14 July 2026 09:49

Two new phishing kits, Jalisco and OmegaLord, have been discovered in attacks targeting Microsoft 365 accounts, using techniques that defeat multi-factor authentication (MFA).

OAuth Client ID Spoofing Lets Attackers Validate Stolen Microsoft Entra Credentials

The Hacker News - 14 July 2026 17:51

At least two distinct threat actors are weaponizing a novel evasion technique called OAuth client ID spoofing in cloud campaigns, while slipping past telemetry. The activity allows users to enumerate user accounts and validate stolen credentials in Microsoft Entra ID environments, without ever generating a successful sign-in event that would otherwise alert defenders.