Scottish Cyber Coordination Centre

Daily Threat Bulletin

27 August 2026

Vulnerabilities

Critical Gitea RCE Actively Exploited as Reported Attack Drops Miner-Like Payload

The Hacker News - 26 August 2026 12:57

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) on Tuesday warned of active exploitation efforts targeting a recently patched critical security flaw impacting Gitea.

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 Vulnerability

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

Hackers target Microsoft SharePoint RCE chain with PoC exploit

BleepingComputer - 26 August 2026 11:47

Attackers are now targeting a chain of two Microsoft SharePoint vulnerabilities that can allow them to execute arbitrary code on unpatched servers, according to threat intelligence company Defused.

Recent Citrix NetScaler Vulnerability Exploited in the Wild

SecurityWeek - 27 August 2026 05:39

CISA is urging government agencies to immediately patch the Citrix NetScaler vulnerability tracked as CVE-2026-8452.

Critical Avada WordPress theme flaw enables zero-click RCE

BleepingComputer - 26 August 2026 18:33

A critical vulnerability chain in the popular Avada theme for WordPress can be exploited by an unauthenticated attacker to execute arbitrary PHP code on the server.

Scottish Cyber Coordination Centre

Ubiquiti patches three max severity security vulnerabilities

BleepingComputer - 26 August 2026 10:17

Ubiquiti has released security patches for three new maximum-severity vulnerabilities that threat actors can exploit remotely without privileges.

Adobe and Nvidia Patch Dozens of Vulnerabilities

SecurityWeek - 26 August 2026 13:39

Adobe and Nvidia each published several advisories, including ones that address critical vulnerabilities in their products.

Chrome 152 Patches Over 300 Vulnerabilities

SecurityWeek - 26 August 2026 10:50

Most of the flaws were discovered by Google using AI, but researchers are still discovering high-value Chrome vulnerabilities.

Threat actors and malware

New GPUThor attack defeats NVIDIA ECC protection for root access

BleepingComputer - 26 August 2026 15:48

A newly disclosed Rowhammer attack called GPUThor can bypass error-correcting code (ECC) protections on NVIDIA GPUs, enabling denial-of-service (DoS) and root-level privilege escalation.

FBI Disrupts China-Linked QTFY Infrastructure Used to Steal Data From U.S. Organizations

The Hacker News - 26 August 2026 23:12

The U.S. Department of Justice (DoJ) on Wednesday announced the disruption of two hacking platforms named QScan and QTRouter operated by Chinese threat actors to target critical infrastructure and other sensitive networks in the country.

Dark Caracal Adds New Malware to Cyber Espionage Arsenal

darkreading - 26 August 2026 22:33

GoCaracal is a new modular malware framework that broadens Dark Caracal's capabilities to steal data and maintain access to victims.