Scottish
Cyber
Coordination
Centre

Daily Threat Bulletin

13 August 2025

Vulnerabilities

Dutch NCSC Confirms Active Exploitation of Citrix NetScaler CVE-2025-6543 in Critical Sectors

The Hacker News - 12 August 2025 15:06

The Dutch National Cyber Security Centre (NCSC-NL) has warned of cyber attacks exploiting a recently disclosed critical security flaw impacting Citrix NetScaler ADC products to breach organizations in the country.

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-2013-3893 Microsoft Internet Explorer Resource Management Errors Vulnerability
CVE-2007-0671 Microsoft Office Excel Remote Code Execution Vulnerability
CVE-2025-8088 RARLAB WinRAR Path Traversal Vulnerability

29,000 Servers Remain Unpatched Against Microsoft Exchange Flaw

Infosecurity Magazine - 12 August 2025 16:00

Over 29,000 Microsoft Exchange servers remain unpatched against a vulnerability that could allow attackers to seize control of entire domains in hybrid cloud environments.

Microsoft August 2025 Patch Tuesday fixes one zero-day, 107 flaws

BleepingComputer - 12 August 2025 14:43

Today is Microsoft's August 2025 Patch Tuesday, which includes security updates for 107 flaws, including one publicly disclosed zero-day vulnerability in Windows Kerberos.

SAP fixed 26 flaws in August 2025 Update, including 4 Critical

Security Affairs - 13 August 2025 01:00

SAP's August 2025 Patch Tuesday released 15 new security notes, including critical fixes, plus four updates to previously released patches.

Adobe Patches Over 60 Vulnerabilities Across 13 Products

SecurityWeek - 13 August 2025 05:36

Adobe's security updates fix vulnerabilities in Commerce, Substance, InDesign, FrameMaker, Dimension and other products.

ICS Patch Tuesday: Major Vendors Address Code Execution Vulnerabilities

SecurityWeek - 13 August 2025 07:36

August 2025 ICS Patch Tuesday advisories have been published by Siemens, Schneider, Aveva, Honeywell, ABB and Phoenix Contact.

Threat actors and malware

Fortinet SSL VPNs Hit by Global Brute-Force Wave Before Attackers Shift to FortiManager

The Hacker News - 12 August 2025 23:35

Cybersecurity researchers are warning of a "significant spike" in brute-force traffic aimed at Fortinet SSL VPN devices. The coordinated activity, per threat intelligence firm GreyNoise, was observed on August 3, 2025, with over 780 unique IP addresses participating in the effort.

Researchers cracked the encryption used by DarkBit ransomware

Security Affairs - 12 August 2025 10:04

Good news for the victims of the DarkBit ransomware, researchers at cybersecurity firm Profero cracked the encryption process, allowing victims to recover files for free without paying the ransom.

Charon Ransomware Emerges With APT-Style Tactics

darkreading - 12 August 2025 15:45

The first documented deployment of the novel malware in a campaign against the Middle Eastern public sector and aviation industry may be tied to China's state-sponsored actor Earth Baxia.

Cybercrime Groups ShinyHunters, Scattered Spider Join Forces in Extortion Attacks on Businesses

The Hacker News - 12 August 2025 22:50

An ongoing data extortion campaign targeting Salesforce customers may soon turn its attention to financial services and technology service providers, as ShinyHunters and Scattered Spider appear to be working hand in hand, new findings show.

UK incidents

Home Office Phishing Scam Targets UK Immigration Sponsors

Infosecurity Magazine - 12 August 2025 15:15

The sophisticated campaign aims to steal credentials of sponsor license holders to facilitate immigration fraud, extortion and other monetization schemes.