Scottish
Cyber
Coordination
Centre

Daily Threat Bulletin

27 August 2025

Vulnerabilities

Citrix Patches Three NetScaler Flaws, Confirms Active Exploitation of CVE-2025-7775

The Hacker News - 26 August 2025 23:59

Citrix has released fixes to address three security flaws in NetScaler ADC and NetScaler Gateway, including one that it said has been actively exploited in the wild.The vulnerabilities in question are listed below -CVE-2025-7775 (CVSS score: 9.2) - Memory overflow vulnerability leading to Remote Code Execution and/or Denial-of-ServiceCVE-2025-7776 (CVSS score: 8.8) - Memory overflow

CISA warns of actively exploited Git code execution flaw

BleepingComputer - 26 August 2025 11:57

The U.S. Cybersecurity & Infrastructure Security Agency (CISA) is warning of hackers exploiting an arbitrary code execution flaw in the Git distributed version control system. [...]

Docker Desktop Vulnerability Leads to Host Compromise

SecurityWeek - 26 August 2025 12:24

A critical vulnerability in Docker Desktop allows attackers to modify the filesystem of Windows hosts to become administrators.The post Docker Desktop Vulnerability Leads to Host Compromise appeared first on SecurityWeek.

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-2025-7775 Citrix NetScaler Memory Overflow Vulnerability.

Threat actors and malware

Silk Typhoon hackers hijack network captive portals in diplomat attacks

BleepingComputer - 26 August 2025 18:33

State-sponsored hackers linked to the Mustang Panda activity cluster targeted diplomats by hijacking web traffic to redirect to a malware serving website. [...]

MixShell Malware Delivered via Contact Forms Targets U.S. Supply Chain Manufacturers

The Hacker News - 26 August 2025 20:00

Cybersecurity researchers are calling attention to a sophisticated social engineering campaign that’s targeting supply chain-critical manufacturing companies with an in-memory malware dubbed MixShell.The activity has been codenamed ZipLine by Check Point Research.

ShadowCaptcha Exploits WordPress Sites to Spread Ransomware, Info Stealers, and Crypto Miners

The Hacker News - 26 August 2025 17:15

A new large-scale campaign has been observed exploiting over 100 compromised WordPress sites to direct site visitors to fake CAPTCHA verification pages that employ the ClickFix social engineering tactic to deliver information stealers, ransomware, and cryptocurrency miners.

UNC6395 and the Salesloft Drift Attack: Why Salesforce OAuth Integrations are a Growing Risk

Security Boulevard - 27 August 2025 00:14

A recent UNC6395 Salesloft Drift breach reveals Salesforce SaaS risks. Learn how to simplify breach detection, prevention, and visibility.The post UNC6395 and the Salesloft Drift Attack: Why Salesforce OAuth Integrations are a Growing Risk appeared first on AppOmni.

Google issued ‘State-backed attack in progress’ warnings after spotting web hijack scheme

The Register - 27 August 2025 05:58

Suspects this was Beijing-backed Typhoon and/or Panda crew targeting diplomats in Asia Google has warned customers of a suspected state-backed attack after observing a web traffic hijacking campaign....