Scottish Cyber Coordination Centre

Daily Threat Bulletin

24 August 2026

Vulnerabilities

GitLab CVE-2026-19478 Comes Under Active Exploitation Within Days of Disclosure

The Hacker News - 21 August 2026 13:34

A newly disclosed security flaw in GitLab has come under active exploitation within days of public disclosure, according to watchTowr. The vulnerability in question is CVE-2026-19478 (CVSS score: 9.4), a case of code injection that allows an unauthenticated attacker to modify or delete publicly accessible GitLab projects and rewrite their data under certain conditions.

CISA orders feds to patch actively exploited TrueConf Server flaws

BleepingComputer - 21 August 2026 09:25

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) ordered U.S. federal agencies to prioritize patching two actively exploited vulnerabilities in the TrueConf Server self-hosted communications platform.

Cisco Patches Nine Crosswork and Secure Workload Flaws, Five Scoring CVSS 10.0

The Hacker News - 21 August 2026 16:33

Cisco has published another round of security updates for Crosswork platforms and Secure Workload Software as part of a continued comprehensive internal security review. Four of the security vulnerabilities affect Crosswork Data Gateway, Crosswork Network Controller, and Crosswork Planning, regardless of the device configuration.

Microsoft patches max severity code execution, privilege escalation flaws

BleepingComputer - 21 August 2026 08:04

Microsoft has patched a maximum-severity vulnerability in the Entra ID identity and access management (IAM) platform that has been exploited in attacks.

Critical Flaw in NASA/JPL Open-Source Spacecraft Command Software Allowed Unauthenticated Command Execution

Security Affairs - 22 August 2026 09:04

Cycode researchers found that AIT-GUI, the browser-based operator console in NASA/JPL open-source AMMOS Instrument Toolkit, shipped with no authentication, no session checks, and no CSRF protection on any of its state-changing endpoints.

Scottish Cyber Coordination Centre

Critical Isolated-vm Vulnerability Leads to RCE on Host

SecurityWeek - 21 August 2026 13:26

The type confusion bug can lead to V8 sandbox escape and control-flow hijacking of the host process.

Threat actors and malware

New SynkLoader malware pushed in Microsoft Teams phishing campaign

BleepingComputer - 21 August 2026 15:01

A previously unknown malware family dubbed SynkLoader is being distributed in Microsoft Teams phishing campaigns to steal credentials via a fake lock screen.

Android Car Malware Spreads Through Built-In Updaters for Ad Fraud, Proxy Botnet

The Hacker News - 21 August 2026 22:11

Kaspersky, which discovered the threat in June 2026, said the end goal of the malware is to serve a multi-stage downloader to enable ad fraud and creation of a proxy botnet.

ToxicPanda Android malware uses VPN permissions to block Google Play

BleepingComputer - 23 August 2026 11:23

The ToxicPanda Android malware has evolved with new malicious functionality, expanding its targeting to 349 applications and adding support for 167 remote commands.

Hackers abuse FTP server banners to deliver new Windows malware

BleepingComputer - 21 August 2026 08:00

Threat actors are abusing FTP banners to hide commands that deliver two previously undocumented remote access trojans named E4del and PINHOLE.

UK incidents

UK Power Plant Disabled for Four Days by Iran-Linked Hackers, Concurrent with US Water Attacks

Security Affairs - 23 August 2026 09:48

Iran-linked hackers shut down a UK power plant for four days in the first confirmed attack of its kind, concurrent with water infrastructure attacks across 12 US states.

Scottish council website carried links to offshore casino sites

BBC News - 21 August 2026 11:57

People looking for information about community councils in the Scottish Borders have instead been directed to online gambling portals.