Scottish Cyber Coordination Centre

Daily Threat Bulletin

21 August 2026

Vulnerabilities

Microsoft Entra ID Flaw (CVSS 10.0) Exploited in Wild, Allows Remote Code Execution

The Hacker News - 21 August 2026 12:36

Microsoft on Thursday warned of a maximum-severity security flaw in Entra ID that it said has been exploited in the wild, but noted that no customer action is required. The vulnerability, tracked as CVE-2026-69836 (CVSS score: 10.0), is a case of remote code execution impacting the tech giant's cloud-based identity and access management service.

Citrix urges admins to patch new NetScaler flaws as soon as possible

BleepingComputer - 20 August 2026 09:14

Citrix has warned customers to immediately secure their systems against two vulnerabilities affecting NetScaler Gateway secure remote access solutions and NetScaler ADC networking appliances.

U.S. CISA adds an MLflow flaw to its Known Exploited Vulnerabilities catalog

Security Affairs - 20 August 2026 09:55

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) added a Progress LoadMaster vulnerability, tracked as CVE-2026-64849 (CVSS score of 9.3), to its Known Exploited Vulnerabilities (KEV) catalog.

Attackers Exploit Zimbra SNMP Flaw for Unauthenticated Remote Code Execution

The Hacker News - 20 August 2026 19:54

A now-patched security flaw impacting Zimbra Collaboration (ZCS) has come under active exploitation in the wild, according to the Polish Computer Emergency Response Team (CERT Polska).

Critical GitLab Flaw Exploited Shortly After Disclosure

SecurityWeek - 20 August 2026 08:48

CVE-2026-19478 can be exploited without authentication to modify or delete public projects and user data.

Critical Elementor Pro bug exposes WordPress sites to RCE attacks

BleepingComputer - 20 August 2026 11:39

A critical vulnerability in the Elementor Pro WordPress plugin could allow attackers to upload executable files for remote code execution on the server.

Scottish Cyber Coordination Centre

Cisco Patches Critical Crosswork, Secure Workload Vulnerabilities

SecurityWeek - 20 August 2026 12:46

The flaws could lead to remote code execution, authentication bypasses, and path traversal attacks.

Atlassian, Splunk Patch Dozens of Critical, High-Severity Vulnerabilities

SecurityWeek - 20 August 2026 13:24

The flaws could be exploited to execute arbitrary code, access sensitive information, and elevate privileges.

Threat actors and malware

Manic: The Android Malware That Exfiltrates Data Even When the Phone Is Offline

Security Affairs - 20 August 2026 19:03

Manic Android malware combines banking fraud and spyware, using a Bluetooth relay to steal data even when devices are offline. ThreatFabric's Mobile Threat Intelligence team has identified a new Android malware, dubbed Manic, which has been active in the wild since at least February 2026.

ToxicPanda 2.0 and GoldDigger Expand Android Banking Attacks with On-Device Fraud

The Hacker News - 20 August 2026 17:08

Cybersecurity researchers have shed light on an updated version of ToxicPanda (aka TgToxic) that comes with "significant enhancements," including a set of 167 remote commands and expands its targeting footprint globally.

Elementor Pro Flaw Could Let Unauthenticated Attackers Upload PHP and Execute Code

The Hacker News - 20 August 2026 12:34

Cybersecurity researchers have disclosed details of a critical flaw in the Elementor Pro WordPress plugin that, if successfully exploited, could lead to remote code execution.The vulnerability, tracked as CVE-2026-32475, carries a CVSS score of 9.0 out of 10.0.