Scottish Cyber Coordination Centre

Daily Threat Bulletin

28 July 2026

Vulnerabilities

Arista patches VeloCloud Orchestrator zero-day exploited in attacks

BleepingComputer - 27 July 2026 19:49

Arista has patched a maximum-severity command injection vulnerability in on-premises VeloCloud Orchestrator deployments that is being actively exploited in attacks. [...]

Public Exploit Released for Patched vBulletin Pre-Auth Code Execution Flaw

The Hacker News - 27 July 2026 21:10

Public exploit details released on July 27 show how an unauthenticated request can reach PHP's eval() function inside vBulletin and execute code on an unpatched forum server. The attack requires no account, administrative access, or interaction from another user.SSD Secure Disclosure lists vBulletin 6.2.1 and earlier, and 6.1.6 and earlier, as affected, but does not give a lower version

'Confused Deputy' Flaws Persist in Google Cloud, Microsoft Azure

darkreading - 27 July 2026 21:57

This category of vulnerabilities allows an attacker to easily acquire administrative level permissions and bypass cloud providers' access controls.

Microsoft Debuts AI Security Platform Built to Find and Fix Software Flaws

Security Boulevard - 27 July 2026 21:51

Microsoft has introduced an AI platform that automates key cybersecurity tasks by combining specialized AI models with AI agents that identify software vulnerabilities and help deploy software patches.

Threat actors and malware

Hackers target US firms in FastJson RCE zero-day attacks

BleepingComputer - 27 July 2026 20:49

Hackers are actively exploiting a vulnerability in the FastJson open-source Java library, allowing remote code execution without user interaction or elevated privileges. [...]

Coca-Cola confirms data theft in Fairlife ransomware attack

BleepingComputer - 27 July 2026 12:39

Scottish Cyber Coordination Centre

The Coca-Cola Company has confirmed that hackers stole data from its dairy subsidiary, Fairlife, during a ransomware attack earlier this month. [...]

Cruciferra Crypter Uses BYOVD and Process Ghosting to Hide Windows Malware

The Hacker News - 27 July 2026 17:21

The China-linked cybercrime group behind the use of income tax-related phishing lures targeting Indian taxpayers, tax professionals, and corporate finance teams has been observed using a sophisticated crypter service called Cruciferra.

TELESHIM Abuses Telegram for C2 in Attacks Against Middle East Governments

The Hacker News - 27 July 2026 15:18

Cybersecurity researchers have flagged fresh malicious cyber activity by a threat actor with ties to East Asia targeting government entities in the Middle East.

Unpatched Fastjson Vulnerability Exploited in Attacks

SecurityWeek - 28 July 2026 08:27

The critical remote code execution bug can be exploited without authentication, under the library's stock default configurations.