Scottish Cyber Coordination Centre

Daily Threat Bulletin

11 June 2026

Vulnerabilities

Microsoft patches Exchange Server zero-day exploited in attacks

BleepingComputer - 10 June 2026 10:44

Microsoft has patched an actively exploited Exchange Server vulnerability that allows threat actors to execute arbitrary JavaScript code in cross-site scripting (XSS) attacks targeting Outlook Web Access users.

Max severity Ivanti Sentry vulnerability now exploited in attacks

BleepingComputer - 11 June 2026 03:20

Attackers are now targeting a recently patched maximum-severity flaw in Ivanti Sentry, enabling them to execute code with root privileges on Internet-exposed secure mobile gateways.

Unpatched Langflow Flaw CVE-2026-5027 Exploited for Unauthenticated RCE

The Hacker News - 10 June 2026 21:30

A high-severity unpatched security flaw in Langflow, an open-source low-code platform to build artificial intelligence (AI) applications, has come under active exploitation in the wild, according to findings from VulnCheck.

New Windows Zero-Day Exploit 'RoguePlanet' Released

SecurityWeek - 10 June 2026 12:44

Exploiting a race condition in Microsoft Defender, the exploit leads to local privilege escalation to SYSTEM.

Critical HVAC and UPS Vulnerabilities Could Let Hackers Disrupt Data Centers

SecurityWeek - 10 June 2026 13:07

Claroty researchers have analyzed the security of Vertiv UPS network cards and the Trane Tracer SC+ HVAC controller.

ServiceNow Patches Vulnerability Exploited Against Some Customers

SecurityWeek - 10 June 2026 10:45

The company updated hosted customer instances to patch a security issue it reportedly had known about since April 7.

Scottish Cyber Coordination Centre

Six Proto6 Vulnerabilities in protobuf.js Expose Node.js Apps to RCE and DoS

The Hacker News - 10 June 2026 11:38

Cybersecurity researchers have flagged half a dozen vulnerabilities in protobuf.js, a JavaScript and TypeScript implementation of Protocol Buffers (Protobuf), that, if successfully exploited, could result in remote code execution (RCE) and denial-of-service (DoS) attacks

Threat actors and malware

GitHub announces npm security changes to tackle supply-chain attacks

BleepingComputer - 10 June 2026 16:41

GitHub has announced that npm v12, expected next month, will introduce several security-focused changes aimed at blocking supply-chain attacks abusing behaviors triggered by the 'npm install' command.

Oracle PeopleSoft servers hacked in ShinyHunters data theft attacks

BleepingComputer - 10 June 2026 15:31

Oracle PeopleSoft servers are being targeted in ongoing data theft attacks by the ShinyHunters extortion gang, which claims to have stolen data from over 100 organizations.

Infostealers Turn Millions of Devices Into Credential Theft Machines

SecurityWeek - 10 June 2026 15:00

As attackers increasingly favor stolen credentials over exploits, infostealers have become a primary source of access for ransomware and other cybercrime operations.

Russian APTs Still Exploiting Patched WinRAR Flaw CVE-2025-8088

Security Affairs - 10 June 2026 14:34

CVE-2025-8088 is a path traversal flaw in WinRAR that lets an attacker write files outside the extraction directory using NTFS Alternate Data Streams. WinRAR fixed it in version 7.13 in July 2025.

China-Linked JDY Botnet Expands to 1,500+ Devices for Cyber Reconnaissance

The Hacker News - 10 June 2026 22:38

Cybersecurity researchers have warned of a "resurgence and expansion" of JDY, a covert network associated with China-nexus state-sponsored threat actors. The JDY botnet comprises over 1,500 SOHO [small office and home office] and IoT devices and operates as a centrally controlled, high-performance scanner used to discover, fingerprint, and continuously map exposed services at scale.