Scottish Cyber Coordination Centre

Daily Threat Bulletin

10 June 2026

Vulnerabilities

CISA Adds Three Known Exploited Vulnerabilities to Catalog

CISA Advisories -

CISA has added three new vulnerabilities to its Known Exploited Vulnerabilities (KEV) Catalog, based on evidence of active exploitation.

CVE-2026-7473 Arista Extensible Operating System Incomplete Comparison with Missing Factors Vulnerability

CVE-2026-11645 Google Chromium V8 Out-of-Bounds Read and Write Vulnerability

CVE-2026-20245 Cisco Catalyst SD-WAN Manager Improper Encoding or Escaping of Output Vulnerability

Ivanti: Max severity Sentry flaw allows code execution as root

BleepingComputer - 10 June 2026 03:26

Ivanti has patched two critical vulnerabilities in its Sentry secure mobile gateway solution, including a maximum-severity flaw that enables remote attackers to execute code with root privileges.

Microsoft Defender 'RoguePlanet' zero-day grants SYSTEM privileges

BleepingComputer - 09 June 2026 20:11

A security researcher has released a new Microsoft Defender zero-day exploit named "RoguePlanet" just hours after Microsoft fixed two previously disclosed flaws during June 2026 Patch Tuesday.

Chrome V8 Zero-Day CVE-2026-11645 Exploited in the Wild - Patch Now

The Hacker News - 09 June 2026 18:28

Google has released security updates to address 74 vulnerabilities, including one that has come under active exploitation in the wild. The high-severity vulnerability, tracked as CVE-2026-11645 (CVSS score: 8.8), has been described as an out-of-bounds memory access in V8, Chrome's JavaScript and WebAssembly engine.

Microsoft Releases Record-Breaking Patch Tuesday With 208 CVEs

Security Affairs - 09 June 2026 23:55

Microsoft Patch Tuesday security updates for June 2026 mark a record. Microsoft shipped fixes for 208 CVEs across Windows, Office, Azure, Exchange, Hyper-V, Secure Boot, BitLocker, and a range of AI tooling.

Scottish Cyber Coordination Centre

SAP fixes critical flaws in NetWeaver and Commerce Cloud

BleepingComputer - 09 June 2026 16:36

SAP has released fixes for 15 vulnerabilities as part of its June 2026 Security Patch package, including four critical-severity flaws affecting SAP NetWeaver and SAP Commerce Cloud.

Critical Veeam RCE Flaw Lets Low-Privilege Users Take Over Backup Servers

Security Affairs - 09 June 2026 17:51

Veeam has patched a critical remote code execution vulnerability, tracked as CVE-2026-44963 (CVSS v4 Score of 9.4), affecting Backup & Replication version 12.x.

LiteLLM Flaw CVE-2026-42271 Exploited in the Wild, Chains to Unauthenticated RCE

The Hacker News - 09 June 2026 12:56

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) on Monday added a high-severity flaw impacting BerriAI LiteLLM to its Known Exploited Vulnerabilities (KEV) catalog, citing evidence of active exploitation.

Adobe Patches 123 Vulnerabilities

SecurityWeek - 09 June 2026 19:20

Nearly half of the security holes, most allowing arbitrary code execution, have been fixed in Adobe's Experience Manager product.

OpenSSL Patches High-Severity Vulnerability Found With AI

SecurityWeek - 09 June 2026 17:47

A total of 18 vulnerabilities have been patched in the latest OpenSSL releases, including many that were potentially discovered by AI.

Threat actors and malware

GitHub disables Microsoft repos pushing password-stealing malware

BleepingComputer - 09 June 2026 12:42

Microsoft removed 73 repositories across its Azure, microsoft, Azure-Samples, and MicrosoftDocs organizations on GitHub, disrupting continuous integration pipelines.

WinRAR Flaw Exploited by Russia-Aligned Groups to Deploy Stealers in Ukraine

The Hacker News - 09 June 2026 18:56

Two Russia-aligned cyber attack campaigns have continued to exploit a security flaw in WinRAR to target Ukrainian organisations, almost a year after patches for the vulnerability were released.

Scottish Cyber Coordination Centre

New FROST Attack Lets Websites Track What Sites and Apps You Open via SSD Timing

The Hacker News - 09 June 2026 16:20

A malicious website can work out which sites you visit and which apps you open, using nothing but JavaScript and the timing of your SSD. The attack, called FROST, needs no native code, no extension, and no permission prompt.

Over 100 NPM, PyPI Packages Hit in New Shai-Hulud Supply Chain Attacks

SecurityWeek - 09 June 2026 12:37

The most recent variants of the self-propagating attacks are named Miasma and Hades.