Scottish Cyber Coordination Centre

Daily Threat Bulletin

10 November 2026

Vulnerabilities

N-able takes cloud platform offline after 30+ “zero-days” published

BleepingComputer - 09 November 2026 17:26

N-able has taken its hosted N-central environments offline and urged on-premises customers to shut down their servers after a security researcher publicly disclosed more than 30 alleged zero-day vulnerabilities, including exploits that could let attackers take over vulnerable systems. [...]

Hackers exploit SSHole OpenSSH flaw to breach Linux systems

BleepingComputer - 09 November 2026 12:04

Hackers are actively exploiting the “SSHole” vulnerability (CVE-2026-123158) in OpenSSH to execute commands, steal credentials, and establish persistent access. [...]

Google Issues Chrome Security Update for Eighth Actively Exploited Zero-Day of 2026

The Hacker News - 10 November 2026 13:22

Google on Monday released updates to patch nine security vulnerabilities, including one that has come under active exploitation in the wild.The high-severity vulnerability, assigned the CVE identifier CVE-2026-125350 (CVSS score: N/A), has been described as a use-after-free bug in the XML component.

CISA Warns of Active Exploitation of OpenSSH, GPUStack, FreeSWITCH, and IBM Flaws

The Hacker News - 10 November 2026 13:01

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) on Monday added four security flaws impacting GPUStack, SignalWire FreeSwitch, OpenBSD OpenSSH, and IBM Aspera Faspex to its Known Exploited Vulnerabilities (KEV) catalog, citing evidence of active exploitation.

Notepad++ 8.9.9 Released With Fixes for 6 Vulnerabilities Allowing Plugin Command Execution

Cyber Security News - 09 November 2026 18:03

Notepad++ released version 8.9.9 on November 6, 2026, fixing six security flaws across Windows message handling, protected file saving, clipboard operations, and MIME Tools decoding. The update addresses flaws including conditional plugin command execution, memory exposure, and buffer overflow.

Scottish Cyber Coordination Centre

QNAP Warns Users as Plex2Shell Flaws Are Used to Hack NAS Devices

Security Affairs - 09 November 2026 15:40

Taiwanese vendor QNAP urges users to update Plex Media Server after reports of NAS compromises through the Plex2Shell vulnerability chain. QNAP urges users to update Plex Media Server through the QNAP App Center after reports that threat actors exploited the Plex2Shell vulnerability chain to compromise NAS devices. “

Microsoft Fixes RCE Bug in Windows Paint After Weeks of Confusion

darkreading - 09 November 2026 22:12

Last month, Microsoft disclosed a vulnerability in Microsoft Paint, but messaging regarding a patch was unclear.

Anthropic’s super bug-finding Mythos model is going into Cisco and IBM products

The Register - 10 November 2026 02:00

Enterprise security tools will offer its capabilities without handing customers the model itself

CISA Adds Four Known Exploited Vulnerabilities to Catalog

CISA Advisories -

CISA has added four new vulnerabilities to its Known Exploited Vulnerabilities (KEV) Catalog, based on evidence of active exploitation. CVE-2026-102895 GPUStack Improper Authentication Vulnerability CVE-2026-116779 SignalWire FreeSwitch Code Injection Vulnerability CVE-2026-123158 OpenBSD OpenSSH Unexpected Status Code or Return Value Vulnerability CVE-2026-123218 IBM Aspera Faspex Incorrect Authorization Vulnerability These types of vulnerabilities are a frequent attack vector for malicious cyber actors and pose significant risks to the federal enterprise.

Threat actors and malware

France blames Iranian hackers for supermarket attacks that sparked fires

BleepingComputer - 09 November 2026 14:32

France has linked October cyberattacks that disrupted refrigeration systems at more than 700 supermarkets and other retail locations to Iranian state-backed hackers, saying the attacks caused food losses and sparked at least 15 fires. […]

Hackers Compromise Ethersphere’s bee-js and Swarm Desktop to Deliver Wallet-Stealing Malware

The Hacker News - 10 November 2026 00:06

Attackers used the Ethersphere project’s own release automation to publish malicious versions of two of its tools for the Swarm decentralized storage network: bee-js 13.3.0 and Swarm Desktop 0.56.2.

Scottish Cyber Coordination Centre

Default ‘admin:admin’ Server Password Helps Researchers Hack Two Automakers, Unlock and Start Cars

The Hacker News - 09 November 2026 17:57

The login systems behind two car brands’ mobile apps could be taken over completely, two security researchers found, allowing them to access any customer’s account and, for an owner with a connected car, unlock the doors and start the engine.

U.S. Agencies Warn Refrigeration Controller Attacks Could Cause Fires and Inventory Losses

The Hacker News - 09 November 2026 12:45

U.S. government agencies have warned that threat actors are actively targeting industrial refrigeration and cold-chain monitoring

RevStealer Uses 100+ Domains and Hijacked YouTube Channels to Spread Credential-Stealing Malware

Cyber Security News - 10 November 2026 08:25

A credential-stealing malware called RevStealer is now spread through more than 100 linked domains, hijacked YouTube channels, and fake AI tools. It targets gamers, content creators, and people who want free software.

Hackers Breach Fireworks AI Through Third-Party Cloud Provider to Steal Customer Data

Cyber Security News - 10 November 2026 06:17

Fireworks AI has disclosed a wider security breach involving customer account details, billing records, datasets, and incomplete model weights. In a November 9, 2026 update, the company said attackers reached its development machines through a third-party cloud provider, expanding the impact beyond the exposed credentials reported in October.

Fake GitHub Security Tools Infect Over 2,000 PCs With Malware

Security Affairs - 09 November 2026 09:07

Fake GitHub security tools are spreading malware that disables defenses, steals sensitive data and infects over 2,000 PCs. Cybersecurity firm Doctor Web has found malware hidden in GitHub projects that look like security tools.