Scottish Cyber Coordination Centre

Daily Threat Bulletin

15 May 2026

Vulnerabilities

Cisco warns of new critical SD-WAN flaw exploited in zero-day attacks

BleepingComputer - 14 May 2026 17:09

Cisco is warning that a critical Catalyst SD-WAN Controller authentication bypass flaw, tracked as CVE-2026-20182, was actively exploited in zero-day attacks that allowed attackers to gain administrative privileges on compromised devices. [...]

CC-4783 - F5 Releases Security Updates for NGINX Vulnerability CVE-2026-42945

NHS Digital - 14 May 2026 15:16

Severity: Medium NGINX Plus and NGINX Open Source have a vulnerability that could force a restart or allow code execution if exploited NGINX Plus and NGINX Open Source have a vulnerability that could force a restart or allow code execution if exploited Updated: 14 May 2026

Hackers exploit auth bypass flaw in Burst Statistics WordPress plugin

BleepingComputer - 14 May 2026 18:07

Hackers are leveraging a critical authentication bypass vulnerability in the WordPress plugin Burst Statistics to obtain admin-level access to websites. [...]

New Fragnesia Linux flaw lets attackers gain root privileges

BleepingComputer - 14 May 2026 04:34

Linux distros are rolling out patches for a new high-severity kernel privilege escalation vulnerability (known as Fragnasia and tracked as CVE-2026-46300) that allows attackers to run malicious code as root. [...]

Broadcom releases VMware Fusion security update for root access bug

Security Affairs - 14 May 2026 16:46

Broadcom patched a high-severity VMware Fusion flaw, CVE-2026-41702, that could let local attackers gain root privileges. Broadcom released a security update for VMware Fusion to address a high-severity vulnerability, tracked as CVE-2026-41702, that could allow local attackers to escalate privileges to root on affected systems.

Mythos Proves Potent in Vulnerability Discovery, Less Convincing Elsewhere

SecurityWeek - 14 May 2026 14:00

Independent benchmarking finds Mythos highly effective for source code audits, reverse engineering, and native-code analysis, though its exploit validation and reasoning capabilities remain inconsistent.

Threat actors and malware

OpenAI confirms security breach in TanStack supply chain attack

BleepingComputer - 14 May 2026 16:07

OpenAI says two employees' devices were breached in the recent TanStack supply chain attack that impacted hundreds of npm and PyPI packages, causing the company to rotate code-signing certificates for its applications as a precaution. [...]

Stealer Backdoor Found in 3 Node-IPC Versions Targeting Developer Secrets

The Hacker News - 14 May 2026 23:52

Cybersecurity researchers are sounding the alarm about what has been described as "malicious activity" in newly published versions of node-ipc.According to Socket and StepSecurity, three different versions of the npm package have been confirmed as malicious - node-ipc@9.1.6node-ipc@9.2.3node-ipc@12.0.1"Early analysis indicates that node-ipc@9.1.6, node-ipc@9.2.3, and node-ipc@12.0.1

ICO Publishes Five-Step Plan to Counter Emerging AI-Powered Attacks

Infosecurity Magazine - 14 May 2026 10:00

The Information Commissioner's Office has released new guidance on how to mitigate the risk of AI-powered attacks