Scottish Cyber Coordination Centre

Daily Threat Bulletin

21 May 2026

Vulnerabilities

CISA Adds Seven Known Exploited Vulnerabilities to Catalog

CISA Advisories -

CISA has added seven new vulnerabilities to its Known Exploited Vulnerabilities (KEV) Catalog, based on evidence of active exploitation.
CVE-2008-4250 Microsoft Windows Buffer Overflow Vulnerability
CVE-2009-1537 Microsoft DirectX NULL Byte Overwrite Vulnerability
CVE-2009-3459 Adobe Acrobat and Reader Heap-Based Buffer Overflow Vulnerability
CVE-2010-0249 Microsoft Internet Explorer Use-After-Free Vulnerability
CVE-2010-0806 Microsoft Internet Explorer Use-After-Free Vulnerability
CVE-2026-41091 Microsoft Defender Elevation of Privilege Vulnerability
CVE-2026-45498 Microsoft Defender Denial of Service Vulnerability

Drupal critical update to fix bug with high exploitation risk

BleepingComputer - 20 May 2026 09:52

Drupal has announced a “core security release” scheduled for later today, warning that threat actors might develop exploits within hours of the update disclosure.

PinTheft: Another Linux Privilege Escalation, Another Working Exploit, This Time Targeting Arch

Security Affairs - 20 May 2026 21:32

PinTheft is a Linux LPE flaw in the RDS subsystem with public exploit code. Arch Linux users face the highest risk and should patch immediately. The wave of Linux local privilege escalation vulnerabilities showing up with working exploit code is not slowing down.

Microsoft Releases Mitigation for YellowKey BitLocker Bypass CVE-2026-45585 Exploit

The Hacker News - 20 May 2026 14:58

Microsoft on Tuesday released a mitigation for a BitLocker bypass vulnerability named YellowKey following its public disclosure last week. The zero-day flaw, now tracked as CVE-2026-45585, carries a CVSS score of 6.8. It has been described as a BitLocker security feature bypass.

Scottish Cyber Coordination Centre

Threat actors and malware

Hackers bypass SonicWall VPN MFA due to incomplete patching

BleepingComputer - 20 May 2026 18:19

Threat actors brute-forced VPN credentials and bypassed multi-factor authentication (MFA) on SonicWall Gen6 SSL-VPN appliances to deploy tools used in ransomware attacks.

Over 320 NPM Packages Hit by Fresh Mini Shai-Hulud Supply Chain Attack

SecurityWeek - 20 May 2026 12:06

A compromised maintainer account was used to publish malicious package versions across the @antv namespace.

GitHub Confirms Hack Impacting 3,800 Internal Repositories

SecurityWeek - 20 May 2026 10:28

The TeamPCP hacking group accessed the repositories after a GitHub employee installed a poisoned VS Code extension.

China-Linked Webworm APT Evolves Tactics, Expands to European Targets

Infosecurity Magazine - 20 May 2026 12:30

China-linked Webworm APT expands beyond Asia, targeting European government organizations and refining its cyber espionage tactics, according to ESET research