Scottish Cyber Coordination Centre

Daily Threat Bulletin

20 April 2026

Vulnerabilities

NIST to stop rating non-priority flaws due to volume increase

BleepingComputer - 19 April 2026 11:17

The National Institute of Standards and Technology will stop assigning severity scores to lower-priority vulnerabilities due to the growing workload from rising submission volumes. [...]

Critical flaw in Protobuf library enables JavaScript code execution

BleepingComputer - 18 April 2026 12:09

Proof-of-concept exploit code has been published for a critical remote code execution flaw in protobuf.js, a widely used JavaScript implementation of Google's Protocol Buffers. [...]

Microsoft Teams right-click paste broken by Edge update bug

BleepingComputer - 18 April 2026 11:11

Microsoft is warning that a recent Microsoft Edge browser update introduced a bug that breaks right-click paste in chats in the Microsoft Teams desktop client. [...]

Microsoft Defender under attack as three zero-days, two of them still unpatched, enable elevated access

Security Affairs - 18 April 2026 07:49

Attackers exploit three Microsoft Defender zero-days, code-named BlueHammer, RedSun, and UnDefend, to gain elevated access. Attackers are exploiting three recently disclosed zero-day flaws in Microsoft Defender to gain higher privileges on compromised systems.

Mirai Variant Nexcorium Exploits CVE-2024-3721 to Hijack TBK DVRs for DDoS Botnet

The Hacker News - 18 April 2026 12:31

Threat actors are exploiting security flaws in TBK DVR and end-of-life (EoL) TP-Link Wi-Fi routers to deploy Mirai-botnet variants on compromised devices, according to findings from Fortinet FortiGuard Labs and Palo Alto Networks Unit 42.

CISA Adds One Known Exploited Vulnerability to Catalog

CISA Advisories -

CISA has added one new vulnerability to its Known Exploited Vulnerabilities (KEV) Catalog, based on evidence of active exploitation. CVE-2026-34197 Apache ActiveMQ Improper Input Validation Vulnerability. This type of vulnerability is a frequent attack vector for malicious cyber actors and poses significant risks to the federal enterprise.

Scottish Cyber Coordination Centre

Threat actors and malware

Payouts King ransomware uses QEMU VMs to bypass endpoint security

BleepingComputer - 17 April 2026 16:10

The Payouts King ransomware is using the QEMU emulator as a reverse SSH backdoor to run hidden virtual machines on compromised systems and bypass endpoint security. [...]

Cyber attacks fuel surge in cargo theft across logistics industry

Security Affairs - 19 April 2026 15:59

Hackers infiltrate logistics firms to steal cargo and divert payments, cyberattacks are linked to organized crime and rising losses. Proofpoint researchers observed crooks targeting trucking and logistics companies, running coordinated remote access campaigns to steal cargo and divert payments.

Hidden VMs: how hackers leverage QEMU to stealthily steal data and spread malware

Security Affairs - 18 April 2026 16:20

Attackers abuse QEMU to hide malware in virtual machines, bypass detection, steal data, and deploy ransomware without leaving any trace. Sophos researchers report a rise in attackers abusing QEMU, an open-source emulator, to hide malicious activity inside virtual machines.

Vercel Breach Tied to Context AI Hack Exposes Limited Customer Credentials

The Hacker News - 20 April 2026 10:05

Web infrastructure provider Vercel has disclosed a security breach that allows bad actors to gain unauthorized access to “certain” internal Vercel systems.The incident stemmed from the compromise of Context.ai, a third-party artificial intelligence (AI) tool, that was used by an employee at the company.

Project Glasswing: When AI Becomes the Ultimate Hacker—and Defender

Security Boulevard - 20 April 2026 05:00

Anthropic has introduced Project Glasswing, a cybersecurity initiative powered by an unreleased AI model called Claude Mythos. This system can identify zero-day vulnerabilities, generate exploits, and even help fix them—often without human input. But there’s a catch: it’s considered too powerful for public release.

UK related

Strengthening cyber resilience across the NHS with collaboration and innovation

NCSC - 17 April 2026 13:00

How the NCSC is reducing risk, improving detection, and helping to keep vital services running.

Scottish
Cyber
Coordination
Centre