



Daily Threat Bulletin

14 May 2026

Vulnerabilities

[New critical Exim mailer flaw allows remote code execution](#)

BleepingComputer - 13 May 2026 17:23

A critical vulnerability affecting certain configurations of the Exim open-source mail transfer agent could be exploited by an unauthenticated remote attacker to execute arbitrary code. [...]

[Windows BitLocker zero-day gives access to protected drives, PoC released](#)

BleepingComputer - 13 May 2026 13:37

A cybersecurity researcher has published proof-of-concept (PoC) exploits for two unpatched Microsoft Windows vulnerabilities named YellowKey and GreenPlasma, which are a BitLocker bypass and a privilege-escalation flaw. [...]

[Microsoft fixes Windows Autopatch bug installing restricted drivers](#)

BleepingComputer - 13 May 2026 11:36

Microsoft has fixed a Windows Autopatch bug that caused driver updates restricted by administrative policies to be deployed on some Autopatch-managed Windows devices in the European Union. [...]

[Microsoft Patch Tuesday for May 2026 fix 138 bugs, some of them are alarming](#)

Security Affairs - 13 May 2026 20:28

Microsoft's May 2026 Patch Tuesday fixed 138 flaws, including 30 critical bugs, across Windows, Office, Azure, Edge, SQL Server, and more. Microsoft's May 2026 Patch Tuesday patched 138 vulnerabilities in a single release. That is a number that gives pause even for people accustomed to these cycles. The affected products span virtually the entire Microsoft [...]

[Quest KACE SMA flaw CVE-2025-32975: when one unpatched tool opens the door to 60 organizations](#)

Security Affairs - 13 May 2026 14:24

CVE-2025-32975 is a critical flaw in Quest KACE SMA used for endpoint management. If exploited, it could impact all managed systems across organizations. CVE-2025-32975 is a critical flaw in Quest KACE SMA used for endpoint management. If exploited, it could impact all managed systems across organizations. Quest KACE SMA is an on-premises endpoint management platform [...]



Scottish
Cyber
Coordination
Centre

Critical Fortinet vulnerabilities fixed in FortiSandbox and FortiAuthenticator

Security Affairs - 13 May 2026 07:22

Fortinet patched critical flaws in FortiSandbox and FortiAuthenticator that could let attackers remotely execute code on unpatched systems. Fortinet addressed two critical vulnerabilities affecting FortiSandbox and FortiAuthenticator. The flaws could allow attackers to execute arbitrary commands or code on unpatched systems.

Microsoft's MDASH AI System Finds 16 Windows Flaws Fixed in Patch Tuesday

The Hacker News - 13 May 2026 20:16

Microsoft has unveiled a new multi-model artificial intelligence (AI)-driven system called MDASH to facilitate vulnerability discovery and remediation at scale, adding that it's being tested by some customers as part of a limited private preview.

Threat actors and malware

Instructure settles with hackers following massive student data theft

Security Affairs - 13 May 2026 11:16

Educational tech firm Instructure reached a deal with hackers after a major Canvas breach exposed data stolen from schools and universities. Educational tech firm Instructure says it reached an agreement with the cybercrime group behind a major Canvas data theft, after attackers broke into its systems and threatened to publish stolen information from schools and [...]

Malware crew TeamPCP open-sources its Shai-Hulud worm on GitHub

The Register - 13 May 2026 09:23

Where it's been well and truly forked, seemingly without Microsoft's code locker noticing

Defending Against China-Nexus Covert Networks of Compromised Devices

CISA Advisories -

Defending against China-nexus covert networks of compromised devices. Explaining the widespread shift in tactics, techniques and procedures (TTPs) towards networks of compromised infrastructure, and how to defend against it.

UK related

UK Cybersecurity Market Expands to £14.7bn with Strong Growth in AI Security Firms

Infosecurity Magazine - 13 May 2026 10:05

UK cybersecurity sector reaches £14.7bn in revenue, driven by rapid growth in AI security firms, increased investment and rising employment across the industry