Scottish Cyber Coordination Centre

Daily Threat Bulletin

15 October 2025

Vulnerabilities

Oracle issued an emergency security update to fix new E-Business Suite flaw CVE-2025-61884

Security Affairs - 14 October 2025 08:31

Oracle released an emergency patch to address an information disclosure flaw, tracked as CVE-2025-61884 (CVSS Score of 7.5), in E-Business Suite's Runtime UI component (versions 12.2.3–12.2.14).

CISA Adds Five Known Exploited Vulnerabilities to Catalog

CISA Advisories -

CISA has added five new vulnerabilities to its Known Exploited Vulnerabilities (KEV) Catalog, based on evidence of active exploitation.
CVE-2016-7836 SKYSEA Client View Improper Authentication Vulnerability.
CVE-2025-6264 Rapid7 Velociraptor Incorrect Default Permissions Vulnerability.
CVE-2025-24990 Microsoft Windows Untrusted Pointer Dereference Vulnerability.
CVE-2025-47827 IGEL OS Use of a Key Past its Expiration Date Vulnerability.
CVE-2025-59230 Microsoft Windows Improper Access Control Vulnerability.

Microsoft October 2025 Patch Tuesday fixes 6 zero-days, 172 flaws

BleepingComputer - 14 October 2025 15:02

Today is Microsoft's October 2025 Patch Tuesday, which includes security updates for 172 flaws, including six zero-day vulnerabilities. Get patching!

Adobe Patches Critical Vulnerability in Connect Collaboration Suite

SecurityWeek - 15 October 2025 05:25

Adobe has published a dozen security advisories detailing over 35 vulnerabilities across its product portfolio.

New SAP NetWeaver Bug Lets Attackers Take Over Servers Without Login

The Hacker News - 15 October 2025 12:06

SAP has rolled out security fixes for 13 new security issues, including additional hardening for a maximum-severity bug in SAP NetWeaver AS Java that could result in arbitrary command execution.

Scottish Cyber Coordination Centre

New Pixnapping Android Flaw Lets Rogue Apps Steal 2FA Codes Without Permissions

The Hacker News - 14 October 2025 17:48

Android devices from Google and Samsung have been found vulnerable to a side-channel attack that could be exploited to covertly steal two-factor authentication (2FA) codes, Google Maps timelines, and other sensitive data without the users' knowledge pixel-by-pixel.

Threat actors and malware

Chinese hackers abuse geo-mapping tool for year-long persistence

BleepingComputer - 14 October 2025 09:28

Chinese state hackers remained undetected in a target environment for more than a year by turning a component in the ArcGIS geo-mapping tool into a web shell.

Researchers Expose TA585's MonsterV2 Malware Capabilities and Attack Chain

The Hacker News - 14 October 2025 11:58

Cybersecurity researchers have shed light on a previously undocumented threat actor called TA585 that has been observed delivering an off-the-shelf malware called MonsterV2 via phishing campaigns.

Researchers warn of widespread RDP attacks by 100K-node botnet

Security Affairs - 14 October 2025 19:20

GreyNoise researchers uncovered a large-scale botnet that is targeting Remote Desktop Protocol (RDP) services in the United States starting on October 8.

UK incidents

UK NCSC Reports 429 cyberattacks in a year, with nationally significant cases more than doubling

Security Affairs - 14 October 2025 12:21

The UK's National Cyber Security Centre (NCSC) reported a record surge in major cyberattacks, responding to 429 incidents from September 2024 to August 2025, including 204 deemed "nationally significant", more than double the previous year.

Senior Execs Falling Short on Cyber-Attack Preparedness, NCSC Warns

Infosecurity Magazine - 14 October 2025 15:30

In a joint warning letter, UK ministers urged FTSE 350 CEOs to bolster cyber defenses.