Scottish Cyber Coordination Centre

Daily Threat Bulletin

6 October 2025

Vulnerabilities

Oracle patches EBS zero-day exploited in Clop data theft attacks

BleepingComputer - 05 October 2025 22:37

Oracle is warning about a critical E-Business Suite zero-day vulnerability tracked as CVE-2025-61882 that allows attackers to perform unauthenticated remote code execution, with the flaw actively exploited in Clop data theft attacks. [...]

Hackers exploited Zimbra flaw as zero-day using iCalendar files

BleepingComputer - 05 October 2025 11:45

Researchers monitoring for larger .ICS calendar attachments found that a flaw in Zimbra Collaboration Suite (ZCS) was used in zero-day attacks at the beginning of the year. [...]

U.S. CISA adds Smartbedded Meteobridge, Samsung, Juniper ScreenOS, Jenkins, and GNU Bash flaws to its Known Exploited Vulnerabilities catalog

Security Affairs - 04 October 2025 16:49

U.S. Cybersecurity and Infrastructure Security Agency (CISA) adds Smartbedded Meteobridge, Samsung, Juniper ScreenOS, Jenkins, and GNU Bash flaws to its Known Exploited Vulnerabilities catalog.

Unauthenticated RCE Flaw Patched in DrayTek Routers

SecurityWeek - 03 October 2025 12:36

The security defect can be exploited remotely via crafted HTTP/S requests to a vulnerable device's web user interface.

Chrome 141 and Firefox 143 Patches Fix High-Severity Vulnerabilities

SecurityWeek - 03 October 2025 09:37

High-severity flaws were patched in Chrome's WebGPU and Video components, and in Firefox's Graphics and JavaScript Engine components.

Quick and Dirty Analysis of Possible Oracle E-Business Suite Exploit Script (CVE-2025-61882), (Mon, Oct 6th)

SANS Internet Storm Centre - 06 October 2025 04:50

This weekend, Oracle published a surprise security bulletin announcing an exploited vulnerability in Oracle E-Business Suite. As part of the announcement, which also included a patch, Oracle published IoC observed as part of the incident response [1].

Scottish Cyber Coordination Centre

Threat actors and malware

Massive surge in scans targeting Palo Alto Networks login portals

BleepingComputer - 04 October 2025 11:18

A spike in suspicious scans targeting Palo Alto Networks login portals indicates clear reconnaissance efforts from suspicious IP addresses, researchers warn. [...]

Reading the ENISA Threat Landscape 2025 report

Security Affairs - 06 October 2025 07:51

ENISA Threat Landscape 2025: Rising ransomware, AI phishing, and state-backed espionage mark a converging, persistent EU cyber threat landscape. ENISA Threat Landscape 2025 report provides a comprehensive analysis of the evolving threat landscape in Europe.

ShinyHunters Launches Data Leak Site: Trinity of Chaos Announces New Ransomware Victims

Security Affairs - 03 October 2025 23:33

Trinity of Chaos, tied to Lapsus$, Scattered Spider & ShinyHunters, hit 39 firms via Salesforce flaws, launching a TOR data leak site. The Trinity of Chaos, a ransomware collective presumably associated with Lapsus$, Scattered Spider, and ShinyHunters groups, launched a Data Leak Site (DLS) on the TOR network containing 39 companies including but not limited [...]

Researchers Warn of Self-Spreading WhatsApp Malware Named SORVEPOTEL

The Hacker News - 03 October 2025 18:32

Brazilian users have emerged as the target of a new self-propagating malware that spreads via the popular messaging app WhatsApp.The campaign, codenamed SORVEPOTEL by Trend Micro, weaponizes the trust with the platform to extend its reach across Windows systems, adding the attack is “engineered for speed and propagation” rather than data theft or ransomware.”SORVEPOTEL has been observed to

UK related

Criminals take Renault UK customer data for a joyride

The Register - 03 October 2025 09:55

Names, numbers, and reg plates exposed in latest auto industry cyber-shunt Renault UK customers are being warned their personal data may be in criminal hands after one of its supplier was hacked....

JLR expected to restart some production after cyber shutdown

BBC News - 06 October 2025 00:14

Work is to resume first at the carmaker’s engine factory in Wolverhampton on Monday.

Scottish Cyber Coordination Centre

The true extent of cyber attacks on UK business - and the weak spots that allow them to happen

BBC News - 06 October 2025 01:52

Are this year's major attacks the "cumulative effect of a kind of inaction on cyber security" from the government and big business?