Scottish
Cyber
Coordination
Centre

Daily Threat Bulletin

14 October 2025

Vulnerabilities

Oracle releases emergency patch for new E-Business Suite flaw

BleepingComputer - 13 October 2025 11:42

Oracle has issued an emergency security update over the weekend to patch another E-Business Suite (EBS) vulnerability that can be exploited remotely by unauthenticated attackers. [...]

Researchers Warn RondoDox Botnet is Weaponizing Over 50 Flaws Across 30+ Vendors

The Hacker News - 13 October 2025 16:42

Malware campaigns distributing the RondoDox botnet have expanded their targeting focus to exploit more than 50 vulnerabilities across over 30 vendors.

Threat actors and malware

Microsoft restricts IE mode access in Edge after zero-day attacks

BleepingComputer - 13 October 2025 18:51

Microsoft is restricting access to Internet Explorer mode in Edge browser after learning that hackers are leveraging zero-day exploits in the Chakra JavaScript engine for access to target devices. [...]

SonicWall VPN accounts breached using stolen creds in widespread attacks

BleepingComputer - 13 October 2025 12:58

Researchers warn that threat actors have compromised more than a hundred SonicWall SSLVPN accounts in a large-scale campaign using stolen, valid credentials. [...]

Google, Mandiant expose malware and zero-day behind Oracle EBS extortion

Security Affairs - 13 October 2025 09:35

Google and Mandiant link Oracle EBS extortion emails to known July-patched flaws and a likely zero-day, CVE-2025-61882. Google Threat Intelligence and Mandiant analyzed the Oracle E-Business Suite extortion campaign, revealing the use of malware.

Stealit Malware spreads via fake game & VPN installers on Mediafire and Discord

Security Affairs - 13 October 2025 08:26

Stealit malware abuses Node.js SEA and Electron to spread via fake game and VPN installers shared on Mediafire and Discord. Fortinet FortiGuard Labs researchers spotted Stealit malware campaign abusing Node.js Single Executable Application (SEA) and sometimes Electron to spread via fake game and VPN installers on Mediafire and Discord.

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.The Proofpoint Threat Research Team described the threat activity cluster as sophisticated, leveraging web injections and filtering checks as part of its attack chains.

NPM Infrastructure Abused in Phishing Campaign Aimed at Industrial and Electronics Firms

SecurityWeek - 13 October 2025 12:40

Threat actors used automation to create over 175 malicious NPM packages targeting more than 135 organizations.

Cyber attack contingency plans should be put on paper, firms told

BBC News - 14 October 2025 00:04

Prepare to switch to off-line systems in the event of a cyber-attack, firms are being advised.

UK related

Ofcom fines 4chan £20K and counting for pretending UK's Online Safety Act doesn't exist

The Register - 13 October 2025 12:10

Regulator warns penalties will pile up until internet toilet does its paperwork Ofcom, the UK's Online Safety Act regulator, has fined online message board 4chan £20,000 ($26,680) for failing to protect children from harmful content....

UK hit by record number of 'nationally significant' cyberattacks

The Record from Recorded Future News - 14 October 2025 01:22