Scottish Cyber Coordination Centre

# Daily Threat Bulletin

13 October 2025

## Vulnerabilities

### Hackers exploiting zero-day in Gladinet file sharing software

BleepingComputer - 10 October 2025 16:08

Threat actors are exploiting a zero-day vulnerability (CVE-2025-11371) in Gladinet CentreStack and Triofox products, which allows a local attacker to access system files without authentication. [...]

### Juniper patched nine critical flaws in Junos Space

Security Affairs - 10 October 2025 15:02

Juniper fixed nearly 220 flaws in Junos OS, Junos Space, and Security Director, including nine critical bugs in Junos Space. Juniper Networks released patches to address nearly 220 vulnerabilities in Junos OS, Junos Space, and Security Director, including nine critical flaws in Junos Space.

### U.S. CISA adds Grafana flaw to its Known Exploited Vulnerabilities catalog

Security Affairs - 10 October 2025 09:27

U.S. Cybersecurity and Infrastructure Security Agency (CISA) adds Grafana flaw to its Known Exploited Vulnerabilities catalog. The U.S. Cybersecurity and Infrastructure Security Agency (CISA) added Grafana flaw, tracked as CVE-2021-43798 (CVSS score 7.5), to its Known Exploited Vulnerabilities (KEV) catalog. Grafana is an open-source platform for monitoring and observability.

### New Oracle E-Business Suite Bug Could Let Hackers Access Data Without Login

The Hacker News - 12 October 2025 23:54

Oracle on Saturday issued a security alert warning of a fresh security flaw impacting its E-Business Suite that it said could allow unauthorized access to sensitive data.The vulnerability, tracked as CVE-2025-61884, carries a CVSS score of 7.5, indicating high severity. It affects versions from 12.2.3 through 12.2.14.

### ZDI Drops 13 Unpatched Ivanti Endpoint Manager Vulnerabilities

SecurityWeek - 10 October 2025 10:45

The unpatched vulnerabilities allow attackers to execute arbitrary code remotely and escalate their privileges.

## Threat actors and malware

Scottish Cyber Coordination Centre

## Attackers exploit valid logins in SonicWall SSL VPN compromise

Security Affairs - 11 October 2025 17:03

Huntress warns of widespread SonicWall SSL VPN breaches, with attackers using valid credentials to access multiple accounts rapidly. Cybersecurity firm Huntress warned of a widespread compromise of SonicWall SSL VPNs, with threat actors using valid credentials to access multiple customer accounts rapidly.

## Ukraine sees surge in AI-Powered cyberattacks by Russia-linked Threat Actors

Security Affairs - 10 October 2025 14:31

Russia-linked actors use AI to craft phishing and malware attacks against entities in Ukraine, says SSSCIP. Russian hackers increasingly use AI in cyberattacks against Ukraine, the country's State Service for Special Communications and Information Protection (SSSCIP) reported.

## Hackers Turn Velociraptor DFIR Tool Into Weapon in LockBit Ransomware Attacks

The Hacker News - 11 October 2025 19:34

Threat actors are abusing Velociraptor, an open-source digital forensics and incident response (DFIR) tool, in connection with ransomware attacks likely orchestrated by Storm-2603 (aka CL-CRI-1040 or Gold Salem), which is known for deploying the Warlock and LockBit ransomware.

## Stealit Malware Abuses Node.js Single Executable Feature via Game and VPN Installers

The Hacker News - 10 October 2025 20:55

Cybersecurity researchers have disclosed details of an active malware campaign called Stealit that has leveraged Node.js' Single Executable Application (SEA) feature as a way to distribute its payloads.

## 175 Malicious npm Packages with 26,000 Downloads Used in Credential Phishing Campaign

The Hacker News - 10 October 2025 17:15

Cybersecurity researchers have flagged a new set of 175 malicious packages on the npm registry that have been used to facilitate credential harvesting attacks as part of an unusual campaign.

## CL0P-Linked Hackers Breach Dozens of Organizations Through Oracle Software Flaw

The Hacker News - 10 October 2025 13:11

Dozens of organizations may have been impacted following the zero-day exploitation of a security flaw in Oracle's E-Business Suite (EBS) software since August 9, 2025, Google Threat Intelligence Group (GTIG) and Mandiant said in a new report released Thursday.