ORACLE E-BUSINESS SUITE ZERO-DAY EXPLOITED IN THE WILD

DAILY SIGNAL

The Core Was Breached

What happened, who's exposed, where it sits, when it hit

- **What:** CVE-2025-61884 = pre-auth SSRF / info disclosure in Oracle Configurator / UiServlet → data access without login.
  - Related: CVE-2025-61882 = pre-auth RCE used in same campaign.
- **Who:** Oracle EBS 12.2.3–12.2.14 (global enterprises; ERP = crown jewels).
- **Where in chain:** ATT&CK T1190 (Exploit Public-Facing App) → initial access → collection/exfil.
- **When:** Exploited before disclosure; Oracle pushed two emergency patches days apart.

From quiet exploitation → emergency patches

- **Early exploitation**, then **late-Sep extortion** emails to execs.
- **Patch #1** (CVE-2025-61882 RCE) → **gap closed**.
- **Patch #2** (CVE-2025-61884 SSRF) → **chain broken**.
- **Active recon** observed shortly after: expect **weaponization lag**.

ERP is the vault. This opens the door.

- **Business:** Mass data theft/extortion, regulatory exposure (PII/finance), reputational shock.
- **Operations:** ERP integrity at risk; finance/HR/supply chain data sensitive by default.
- **Security:** 0-day campaign shows direct exploitation of core apps—no phish needed.

The Bigger Game: What Comes Next

Dearest executive,

We are CL0P team. If you haven't heard about us, you can google about us on internet.

We have recently breached your Oracle E-Business Suite application and copied a lot of documents.
All the private files and other information are now held on our systems.

But, don't worry. You can always save your data for payment. We do not seek political power or care about any business.
So, your only option to protect your business reputation is to discuss conditions and pay claimed sum.
In case you refuse, you will lose all abovementioned data: some of it will be sold to the black actors, the rest will be published on our blog and shared on torrent trackers.

We always fulfil all promises and obligations.

We have carefully examined the data we got. And, regrettably for your company, this analysis shows that estimated financial losses, harm to reputation , and regulatory fines are likely to materially exceed the amount claimed.

Lower you see our contact email addresses:
support@pubstorm.com
support@pubstorm.net

As evidence, we can show any 3 files you ask or data row.
We are also ready to continue discussing the next steps after you confirm that you are a legitimate representative of the company.
We are not interested in destroying your business. We want to take the money and you not hear from us again.
Time is ticking on clock and in few days if no payment we publish and close chat.
Please convey this information to your executive and managers as soon as possible.
After a successful transaction and receipt of payment we promise

1) technical advice
2) We will never publish you data
3) Everything we download will be delete w/proof
4) Nothing will ever disclose

Decide soon and recall that no response result in blog posting. Name is first and soon data after. We advice not reach point of no return.

KR CL0P

- **Patch both**: 61882 (RCE) + 61884 (SSRF). Ensure Oracle prerequisites are met.
- **De-expose EBS**: pull management/UI off the internet; put behind VPN/IdP.
- **WAF block** (temp): deny */OA_HTML/SyncServlet* & */configurator/UiServlet*.
- **Rotate secrets** tied to EBS (DB, app, API keys).
- **Hunt logs** for odd UiServlet/SyncServlet calls, reverse shells, unusual egress.
- **Monitor:** add detections (SIEM/IDS) + alert on new admin users/config edits.

Under the hood: UiServlet SSRF → data access; SyncServlet → RCE

- Entry: GET/POST /OA_HTML/configurator/UiServlet?return_url=... (unsanitized/redirected target) → SSRF to internal resources; pre-auth.
- Effect: Read internal endpoints / metadata → data exposure; staging for follow-on RCE.
- Chain: SSRF (61884) used in leaked PoC; RCE (61882) used in Cl0p attacks (/OA_HTML/SyncServlet).
- Artifacts to hunt:
  - Web logs: unusual UiServlet / SyncServlet hits (odd referrers, long query strings, off-hours).
  - Host: bash -i >& /dev/tcp/... patterns; unexpected outbound to rare IPs.
  - Files: odd .jsp/.class in webroot; droppers (e.g., server.py, temp archives).
- ATT&CK mapping: T1190 (Exploit Public-Facing App) → Collection (T1119) → Exfil (T1041).Code boxes (small, for slide):
- WAF rule (conceptual): Block paths */OA_HTML/SyncServlet* & */configurator/UiServlet*.
- SIEM seeds:
  - “uri_path=*/OA_HTML/*Servlet* AND (status=200 OR 302) AND NOT src_ip in allowlist”
  - “message=("bash -i" OR "/dev/tcp/") host=ebs*”

From eCrime to geo-economics: why ERP is the new prize

- **ClOp playbook:** zero-day → mass extortion (MOVEit → EBS): scale over stealth.
- **Business readout:** Boardroom risk = data governance, audit, insurance, brand trust, SEC/DPAs.
- **Market impact:** More vendor due diligence, SBOM/attestation, secure build scrutiny.
- **Policy arc:** Expect tougher procurement baselines; faster mandated patch SLAs; “trusted tech” blocs.

•**Moves:** Isolate EBS; rotate creds; image + re-deploy; legal & PR ready.

What happens next (0–365 days)

0-30 days

Containment: Quiet extortion; data staging; attackers test more endpoints.

- **Signals:** Exec extortion emails; spikes in EBS egress; UiServlet anomalies.
- **Moves:** Isolate EBS; rotate creds; image + re-deploy; legal & PR ready.

30-90 days

Public & Reg: Leak site posts; customer/legal notifications; audits.

- **Signals:** DLP hits, media inquiries, partner alerts.
- **Moves:** Breach disclosures; regulator liaison; compensating controls; tabletop lessons.

90-365 days

Aftershocks: Lawsuits; contract reviews; cyber insurance shifts; vendor hardening.

- **Signals:** Renewal frictions; audit findings; premium increases.
- **Moves:** Always-on patch cadence, private access gateway for ERP, continuous detection content.

DAILY SIGNAL

Breaches, exploits, threat actors — decoded for you, daily