INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-29 15:06 UTC

CVE-2025-61882: Critical Oracle E-Business Suite 0-Day Actively Exploited by Cl0p Ransomware Group

CVE VULNERABILITY | **CRITICAL** | CVSS 9.8

SCC Item ID	SCC-CVE-2026-0370
Type	CVE Vulnerability
CVE ID	CVE-2025-61882
Severity	CRITICAL
CVSS Base Score	9.8
EPSS Score	0.9972 (100th percentile)
Affected Products	Oracle E-Business Suite (specific versions not confirmed from available source data; Oracle Security Alert advisory references CVE-2025-61882)
Published	3 hours ago
Discovery Source	Serper

Executive Summary

A critical zero-day vulnerability in Oracle E-Business Suite (CVE-2025-61882) is under active exploitation in the wild, with the Cl0p ransomware group attributed to account takeover activity against affected organizations, according to Rapid7, BleepingComputer, and Halcyon. Oracle has issued a Security Alert Advisory for the vulnerability, which carries a CVSS base score of 9.8. Organizations running Oracle E-Business Suite face immediate risk of account compromise, data theft, and ransomware deployment until the Oracle-issued patch is applied.

Technical Analysis

CVE-2025-61882 is a critical zero-day affecting Oracle E-Business Suite, with a CVSS base score of 9.8 and an EPSS score of 0.99722 (99.95th percentile), indicating near-certain exploitation probability. Rapid7's emergency threat response (ETR) confirms in-the-wild exploitation. Halcyon attributes exploitation activity to the Cl0p ransomware group, specifically for account takeover (MITRE T1078, Valid Accounts) consistent with Cl0p's established pattern of exploiting enterprise application vulnerabilities for initial access (T1190, Exploit Public-Facing Application). BleepingComputer has independently confirmed exploitation in attacks. Oracle issued a dedicated Security Alert Advisory at oracle.com/security-alerts/alert-cve-2025-61882.html. Specific affected version ranges, CWE classification, CVSS vector string, and precise technical attack mechanics are not

confirmed from the sources available during this analysis; the Oracle advisory and NVD entry (nvd.nist.gov/vuln/detail/CVE-2025-61882) are the authoritative references for those details. CISA KEV listing status was not confirmed at time of analysis; check cisa.gov/known-exploited-vulnerabilities for current status.

Action Checklist

1. Step 1: Containment, Immediately restrict external network access to Oracle E-Business Suite instances. Place E-Business Suite behind a web application firewall or restrict access to trusted IP ranges while the patch is obtained and staged. Review the Oracle Security Alert Advisory at oracle.com/security-alerts/alert-cve-2025-61882.html for any available workarounds applicable before patching.
2. Step 2: Detection, Review Oracle E-Business Suite authentication and access logs for anomalous account activity consistent with T1078 (Valid Accounts): unexpected logins from unusual IP ranges, off-hours access, creation of new accounts or privilege escalation events, and bulk data access patterns. Cross-reference user session logs against known Cl0p infrastructure IOCs if available from threat intelligence feeds (consult Rapid7 ETR and Halcyon report for any published indicators; at time of analysis, specific IOCs were not confirmed in primary sources). Check for unauthorized modifications to E-Business Suite user account configurations. NIST AU-6 (Audit Record Review, Analysis, and Reporting) applies; prioritize log review for the period from initial public disclosure forward.
3. Step 3: Eradication, Apply the patch referenced in the Oracle Security Alert Advisory for CVE-2025-61882 as the primary remediation. Verify the patch applies to your specific E-Business Suite version by consulting the Oracle advisory directly; do not infer version coverage from secondary sources. Reset credentials for all E-Business Suite accounts, particularly privileged and service accounts, consistent with D3-CRO (Credential Rotation) and D3-CH (Credential Hardening). Disable or remove any accounts not confirmed as legitimate per CIS 5.3 (Disable Dormant Accounts) and CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts).
4. Step 4: Recovery, After patching, validate that the Oracle E-Business Suite instance no longer exhibits the exploitable condition per Oracle's post-patch verification guidance. Re-enable access incrementally, monitoring for resumed anomalous activity. Enforce MFA for all E-Business Suite accounts consistent with CIS 6.3 (Require MFA for Externally-Exposed Applications) and D3-MFA (Multi-factor Authentication). Review NIST AC-6 (Least Privilege) posture across E-Business Suite user roles; remove excess permissions surfaced during the account review in Step 3.
5. Step 5: Post-Incident, Document gaps exposed by this event: was the E-Business Suite instance inventoried per CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory)? Were patch response SLAs defined for critical vendor security alerts? Evaluate whether existing vulnerability management processes (CIS 7.1, CIS 7.2) include Oracle Security Alert Advisories in scope. Review NIST AC-2 (Account Management) compliance for E-Business Suite, focusing on provisioning controls that would limit Cl0p-style account takeover impact.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE

Escalation Criteria	Escalate immediately to CISO, legal counsel, and executive leadership if forensic review of FND_LOGINS or OHS access logs confirms unauthorized authentication events against Oracle EBS, as successful exploitation by Cl0p enabling access to EBS financial, HR, or customer data constitutes a potential data breach triggering regulatory notification obligations under GDPR, CCPA, HIPAA, or PCI DSS depending on data classification of EBS content.
Recovery Notes	After patching and credential rotation, maintain elevated monitoring of Oracle EBS OHS access logs and FND_LOGINS for a minimum of 30 days, as Cl0p is known to establish persistence and delay ransomware deployment to maximize dwell time and data exfiltration volume before encrypting. Validate post-patch integrity by confirming the AD patch history entry for the CVE-2025-61882 fix and performing a test authentication cycle from a controlled external IP to confirm the bypass condition is resolved. Monitor Oracle concurrent manager and database scheduler jobs weekly during the recovery window for any Cl0p-staged exfiltration jobs that may have been pre-scheduled prior to eradication.
Forensic Artifacts	Oracle OHS/Apache access logs ($INST_TOP/logs/ora/10.1.3/Apache/access_log): POST requests to /OA_HTML/AppsLogin and /OA_HTML/RF.jsp from non-organizational source IPs during the exploitation window are the primary indicator of CVE-2025-61882 authentication bypass attempts by Cl0p. \| Oracle FND_LOGINS and FND_USER database tables: rows with CREATION_DATE or LAST_UPDATE_DATE falling within the exploitation window and USER_NAME values not matching HR-provisioned accounts indicate attacker-created or hijacked accounts consistent with Cl0p account takeover methodology. \| Oracle FND_CONCURRENT_REQUESTS table and concurrent manager logs ($APPLCSF/$APPLLOG/): large-volume data export requests (e.g., against AR, AP, HR, or GL modules) submitted during off-hours by recently-created or anomalous accounts indicate Cl0p pre-ransomware data staging activity. \| OS-level memory image of the EBS application tier server (captured via LiME or WinPmem before containment actions): may contain in-memory artifacts of the exploit payload, injected code, or Cl0p ransomware staging components that are not present in on-disk forensics. \| Oracle Database alert log ($ORACLE_BASE/diag/rdbms///trace/alert_.log) and OS authentication logs (/var/log/secure or /var/log/auth.log): correlated timestamps between ORA- errors, unusual database connection spikes, and OS-level su/sudo events can establish the exploitation-to-lateral-movement timeline specific to this Cl0p campaign.

Per-Action IR Details

Step 1: Containment — Immediately restrict external network access to Oracle E-Business Suite instances. Place E-Business Suite behind a web application firewall or restrict access to trusted IP ranges while the patch is obtained and staged. Review the Oracle Security Alert Advisory at oracle.com/security-alerts/alert-cve-2025-61882.html for any available workarounds applicable before patching.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy: isolate affected systems to prevent further exploitation while preserving forensic state and maintaining business continuity where possible.

Controls: NIST AC-4 (Information Flow Enforcement), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 4.5 (Implement and Manage a Firewall on End-User Devices)

Compensating: If no WAF is available, use host-based iptables/nftables rules or Windows Firewall to restrict inbound TCP/443 and TCP/8000–8090 (default Oracle EBS ports) to an allowlist of trusted source IPs. On Linux: `iptables -I INPUT -p tcp --dport 443 -j DROP` followed by explicit ACCEPT rules for trusted CIDRs. Verify with `iptables -L -n -v`. Document all blocked ranges in a timestamped change log for the post-incident review.

Evidence: Before restricting network access, capture active network state to preserve evidence of any ongoing Cl0p C2 connections or lateral movement from the EBS host: run `netstat -ano` (Windows) or `ss -tulnp` / `netstat -tulnp`

(Linux) and save full output with timestamp. Capture `arp -a` and active routing tables. On Linux, run `ss -s` for socket summary. These volatile connection records are destroyed the moment firewall rules drop active sessions. Also capture `/var/log/httpd/access_log` and Oracle EBS Apache/OHS access logs (default path: `$INST_TOP/logs/ora/10.1.3/Apache/access_log`) before any network change truncates ongoing write activity.

Step 2: Detection — Review Oracle E-Business Suite authentication and access logs for anomalous account activity consistent with T1078 (Valid Accounts): unexpected logins from unusual IP ranges, off-hours access, creation of new accounts or privilege escalation events, and bulk data access patterns. Cross-reference user session logs against known Cl0p infrastructure IOCs. Check for unauthorized modifications to E-Business Suite user account configurations. NIST AU-6 (Audit Record Review, Analysis, and Reporting) applies; prioritize log review for the period from initial public disclosure forward.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis: correlate log sources to establish scope of compromise, identify attacker-created accounts, and determine initial access timeline relative to CVE-2025-61882 public disclosure.

Controls: NIST AU-6 (Audit Record Review, Analysis, And Reporting), NIST AU-3 (Content Of Audit Records), CIS 8.2 (Collect Audit Logs)

Compensating: Without a SIEM, query Oracle EBS FND_LOGINS and FND_USER tables directly via SQL to identify accounts created or modified after the CVE disclosure date: `SELECT USER_NAME, CREATION_DATE, LAST_UPDATE_DATE, LAST_LOGON_DATE FROM FND_USER WHERE CREATION_DATE > SYSDATE - 30 OR LAST_UPDATE_DATE > SYSDATE - 30 ORDER BY LAST_UPDATE_DATE DESC;`. For OS-level log review, use `grep` against Oracle OHS access logs filtering for POST requests to `/OA_HTML/AppsLogin` or `/OA_HTML/RF.jsp` from non-RFC1918 source IPs. Use `awk '{print $1}' access_log | sort | uniq -c | sort -rn | head -50` to surface high-frequency source IPs for IOC cross-reference against published Cl0p infrastructure lists (check CISA advisories and Feodo Tracker).

Evidence: The primary forensic artifacts for CVE-2025-61882 account takeover activity are: (1) Oracle EBS OHS/Apache access logs at `$INST_TOP/logs/ora/10.1.3/Apache/access_log` — look for POST requests to authentication endpoints from anomalous source IPs; (2) Oracle FND_LOGINS table entries showing session initiations outside business hours or from IPs not matching the organization's known user population; (3) Oracle FND_USER_RESP_GROUPS_DIRECT and FND_GRANTS tables for unexpected privilege assignments made during the exposure window; (4) Oracle Alert Log at `$ORACLE_BASE/diag/rdbms///trace/alert_.log` for database-level anomalies coinciding with exploitation; (5) OS authentication logs — `/var/log/secure` (RHEL/CentOS) or `/var/log/auth.log` (Ubuntu) — for OS-level account activity on the EBS application tier host that may indicate post-exploitation lateral movement by Cl0p.

Step 3: Eradication — Apply the patch referenced in the Oracle Security Alert Advisory for CVE-2025-61882 as the primary remediation. Verify the patch applies to your specific E-Business Suite version by consulting the Oracle advisory directly; do not infer version coverage from secondary sources. Reset credentials for all E-Business Suite accounts, particularly privileged and service accounts, consistent with D3-CRO (Credential Rotation) and D3-CH (Credential Hardening). Disable or remove any accounts not confirmed as legitimate per CIS 5.3 (Disable Dormant Accounts) and CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts).

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication: remove the vulnerability and all attacker-introduced artifacts (unauthorized accounts, implanted credentials, staged ransomware components) before restoring service.

Controls: NIST AC-2 (Account Management), NIST AC-6 (Least Privilege), CIS 5.3 (Disable Dormant Accounts), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts), CIS 7.3 (Perform Automated Operating System Patch Management), CIS 7.4 (Perform Automated Application Patch Management)

Compensating: For credential reset without an identity management platform, use Oracle EBS FNDCPASS utility to bulk-reset application account passwords: `FNDCPASS apps/ 0 Y system/ USER `. For service accounts, update corresponding Oracle Wallet or `dbc` file credentials and restart application tier services. To enumerate all active EBS

accounts for review prior to disabling: `SELECT USER_NAME, START_DATE, END_DATE, LAST_LOGON_DATE FROM FND_USER WHERE NVL(END_DATE, SYSDATE+1) > SYSDATE ORDER BY LAST_LOGON_DATE DESC NULLS LAST;`. Flag any account with NULL LAST_LOGON_DATE and CREATION_DATE within the exploitation window as high-priority for disabling.

Evidence: CRITICAL — volatile evidence must be captured BEFORE patching, credential rotation, or account deletion, as these actions destroy live attacker state. Before executing this step: (1) acquire a full memory image of the EBS application server using LiME (Linux) or WinPmem (Windows) to preserve any in-memory Cl0p staging artifacts or injected code; (2) capture running process list with full command-line arguments via `ps auxf` (Linux) or `Get-WmiObject Win32_Process | Select ProcessId, ParentProcessId, Name, CommandLine` (Windows); (3) export the current FND_USER table and FND_LOGINS table to flat files before any account modifications; (4) collect any Oracle EBS concurrent request logs from `$APPLCSF/$APPLLOG/` that may show bulk data export jobs (Cl0p commonly stages data exfiltration via scheduled database exports before deploying ransomware); (5) image the Oracle EBS `$APPL_TOP` directory listing with timestamps (`find $APPL_TOP -newer /tmp/baseline.txt -ls > /tmp/modified_files.txt`) to identify any files tampered with during the exploitation window.

Step 4: Recovery — After patching, validate that the Oracle E-Business Suite instance no longer exhibits the exploitable condition per Oracle's post-patch verification guidance. Re-enable access incrementally, monitoring for resumed anomalous activity. Enforce MFA for all E-Business Suite accounts consistent with CIS 6.3 (Require MFA for Externally-Exposed Applications) and D3-MFA (Multi-factor Authentication). Review NIST AC-6 (Least Privilege) posture across E-Business Suite user roles; remove excess permissions surfaced during the account review in Step 3.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery: restore systems to verified clean state, confirm the vulnerability is remediated, and harden configuration to prevent recurrence before returning to full production.

Controls: NIST AC-6 (Least Privilege), NIST AC-17 (Remote Access), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.5 (Require MFA for Administrative Access)

Compensating: If Oracle-native MFA integration is not yet licensed or configured, enforce MFA at the network perimeter by requiring all EBS access to route through a VPN gateway with MFA (e.g., OpenVPN with TOTP via Google Authenticator PAM module) as an interim control. For patch validation without access to Oracle's verification tooling, confirm the patch application by checking the Oracle Applications DBA (AD) patch history: query `SELECT PATCH_NAME, PATCH_TYPE, END_DATE FROM AD_APPLIED_PATCHES WHERE PATCH_NAME LIKE '%%' ORDER BY END_DATE DESC;`. Additionally, replay a safe proof-of-concept request pattern from the advisory (if published) against the patched instance in a staging environment to confirm the vulnerable code path returns an error rather than authentication bypass.

Evidence: Before re-enabling external access, verify no Cl0p persistence mechanisms remain: check Oracle EBS concurrent manager job queue (`FND_CONCURRENT_REQUESTS`) for any scheduled jobs created during the exploitation window that could re-exfiltrate data post-recovery; review Oracle Database scheduler jobs via `SELECT JOB_NAME, OWNER, ENABLED, LAST_START_DATE FROM DBA_SCHEDULER_JOBS ORDER BY LAST_START_DATE DESC;`; confirm no unauthorized OS-level cron jobs or systemd timers were introduced on the application tier host (`crontab -l -u oracle`, `ls -la /etc/cron*`, `systemctl list-timers`). Capture a clean baseline snapshot of FND_USER and privilege tables post-remediation for comparison during the monitoring window.

Step 5: Post-Incident — Document gaps exposed by this event: was the E-Business Suite instance inventoried per CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory)? Were patch response SLAs defined for critical vendor security alerts? Evaluate whether existing vulnerability management processes (CIS 7.1, CIS 7.2) include Oracle Security Alert Advisories in scope. Review NIST AC-2 (Account Management) compliance for E-Business Suite, focusing on provisioning controls that would limit Cl0p-style account takeover impact.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity: conduct lessons-learned review, update detection capabilities, and improve processes to reduce dwell time and blast radius for future Cl0p or similar ransomware group campaigns

targeting Oracle EBS.

Controls: NIST AC-2 (Account Management), NIST AU-6 (Audit Record Review, Analysis, And Reporting), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: For teams without a formal vulnerability management platform, establish a lightweight Oracle Security Alert monitoring process: create a free RSS feed subscription or weekly manual check of `oracle.com/security-alerts/` and log each advisory in a shared spreadsheet with fields for CVE ID, affected product/version, CVSS score, patch availability date, and assigned remediation owner with SLA due date. For asset inventory validation, use `nmap -sV -p 8000-8090,443,80 ` to rediscover Oracle EBS instances that may not be formally documented, and cross-reference results against the CMDB.

Evidence: For the lessons-learned record, preserve and attach: (1) the full timeline reconstructed from OHS access logs and FND_LOGINS showing first evidence of CVE-2025-61882 exploitation versus the Oracle advisory publication date — this delta is the organization's effective exposure window; (2) a list of all FND_USER accounts created, modified, or accessed anomalously during the incident window, annotated with whether each was a legitimate account or attacker-created; (3) any Cl0p-associated IOCs (IPs, user-agents, URI patterns) observed in EBS logs, formatted as STIX 2.1 indicators for sharing with ISAC peers if applicable; (4) documentation of whether Oracle EBS was present in the asset inventory prior to this event, to substantiate the CIS 1.1 gap finding with evidence rather than assertion.

Detection Guidance

Focus detection on Oracle E-Business Suite authentication and session logs for indicators of T1078 (Valid Accounts abuse) and T1190 (exploitation of public-facing application). Specific patterns to query: (1) Authentication events from IP addresses outside expected organizational ranges, particularly during off-hours. (2) Accounts with no prior login history suddenly authenticating successfully, possible indicator of account creation or takeover via the vulnerability. (3) Privilege escalation events or role assignment changes in E-Business Suite administrative logs. (4) Bulk or unusual query patterns against E-Business Suite data modules, particularly HR, financial, or procurement data consistent with Cl0p pre-exfiltration reconnaissance. (5) New service accounts or API credentials created after the vulnerability disclosure date. Apply NIST AU-6 (Audit Record Review) and AU-12 (Audit Record Generation) controls; confirm logging is active across all E-Business Suite tiers. D3-LAM (Local Account Monitoring) and D3-UAP (User Account Permissions) techniques are directly applicable. Consult the Rapid7 ETR (rapid7.com/blog/post/etr-cve-2025-61882-critical-0day-in-oracle-e-business-suite-exploited-in-the-wild/) and Halcyon report for any published indicators of compromise.

Indicators of Compromise

Type	Value	Context	Confidence
URL	`https://www.rapid7.com/blog/post/etr-cve-2025-61882-critical-0day-in-oracle-e-business-suite-exploited-in-the-wild/`	Rapid7 Emergency Threat Response — primary technical source; check for updated IOC list	HIGH
URL	`https://www.halcyon.ai/ransomware-research-reports/security-alert-cl0p-abuses-oracle-e-business-suite-for-account-takeover`	Halcyon attribution report linking Cl0p to CVE-2025-61882 account takeover activity; check for infrastructure IOCs	MEDIUM

Framework Mappings

MITRE-ATTACK

- **T1190** — Exploit Public-Facing Application
- **T1078** — Valid Accounts

NIST-800-53R5

- **CA-8** — Penetration Testing
- **RA-5** — Vulnerability Monitoring and Scanning
- **SC-7** — Boundary Protection
- **SI-2** — Flaw Remediation
- **SI-7** — Software, Firmware, and Information Integrity
- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **CP-9** — System Backup
- **IR-4** — Incident Handling
- **SI-4** — System Monitoring
- **IR-5** — Incident Monitoring

NIST-CSF-2

- **RS.MI-01** — Incidents are contained
- **DE.AE-08** — Incidents are declared when adverse events meet the defined incident criteria

HIPAA-SECURITY

- **164.308(a)(7)(ii)(A)** — Data Backup Plan

ISO-27001-2022

- **A.5.29** — Information security during disruption
- **A.8.8** — Management of technical vulnerabilities

CIS-V8

- **8.2** — Collect Audit Logs

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1190	Exploit Public-Facing Application	Initial-Access
T1078	Valid Accounts	Defense-Evasion

Sources

Source	URL	Tier
Linkedin	https://www.linkedin.com/pulse/warning-threat-actors-exploit-critic...	T3
(consolidated)	https://www.bleepingcomputer.com/news/security/new-oracle-e-busines...	T2
Critical 0day in Oracle E-Business Suite exploited in-the-wild - Rapid7	https://www.rapid7.com/blog/post/etr-cve-2025-61882-critical-0day-i...	T1
Cl0p Abuses Oracle E-Business Suite for Account Takeover - Halcyon	https://www.halcyon.ai/ransomware-research-reports/security-alert-c...	T3
Oracle Security Alert Advisory - CVE-2025-61882	https://www.oracle.com/security-alerts/alert-cve-2025-61882.html	T1
NVD	https://nvd.nist.gov/vuln/detail/CVE-2025-61882	T1

Generated 2026-06-29 15:06 UTC by TJS Security Command Center