INTELLIGENCE BRIEFING
Security Command Center

TLP:CLEAR
2026-03-29 18:41 UTC

Madison Square Garden Data Breach Linked to Oracle EBS Exploitation Campaign

DATA BREACH | HIGH | CVSS 8.1

SCC Item ID	SCC-DBR-2026-0059
Type	Data Breach
Severity	HIGH
CVSS Base Score	8.1
Affected Products	Oracle E-Business Suite (EBS), Madison Square Garden Entertainment Corp. deployment; specific version not publicly confirmed
Published	2026-03-03
Discovery Source	Serper

Executive Summary

Madison Square Garden Entertainment Corp. has confirmed a data breach stemming from a broader 2025 exploitation campaign targeting Oracle E-Business Suite (EBS) deployments across multiple organizations. Attackers exfiltrated employee and organizational data, with MSG disclosing the incident months after the initial compromise occurred. Organizations running Oracle EBS face elevated risk of undetected data theft; delayed discovery timelines suggest threat actors maintained persistent access before exfiltration was identified.

Technical Analysis

The breach is linked to a 2025 campaign targeting Oracle E-Business Suite (EBS) environments across multiple victim organizations. The specific CVE identifier(s) exploited have not been publicly confirmed in available sources as of this analysis. The attack chain maps to MITRE ATT&CK techniques T1190 (Exploit Public-Facing Application), T1078 (Valid Accounts), T1213 (Data from Information Repositories), and T1567 (Exfiltration Over Web Service). The underlying weakness is classified under CWE-284 (Improper Access Control). Specific Oracle EBS version(s) affected at MSG have not been publicly disclosed. No CVE-specific CVSS or EPSS data is available for this campaign vector at time of analysis. Patch status for the exploitation vector cannot be confirmed pending CVE identification. Attribution to a named threat actor has not been publicly established. Source quality for this item is limited (all available sources are Tier 3 news outlets); technical details should be treated as preliminary pending additional disclosure from Oracle or MSG.

Action Checklist

1. Step 1, Inventory: Identify all Oracle EBS deployments in your environment, including version, patch level, and network exposure. Prioritize internet-facing or DMZ-adjacent instances.
2. Step 2, Patch Review: Cross-reference your Oracle EBS patch level against Oracle's January and April 2025 Critical Patch Update advisories. Apply any outstanding patches, with priority on authentication and access control fixes.
3. Step 3, Access Audit: Review Oracle EBS user accounts for signs of account misuse or creation of unauthorized accounts (T1078). Disable or rotate credentials for privileged accounts with no recent legitimate activity.
4. Step 4, Log Review: Pull Oracle EBS application logs, database audit logs, and network egress logs for the past 90 days. Look for anomalous data access patterns against HR, payroll, and organizational data repositories (T1213) and large or unusual outbound transfers (T1567).
5. Step 5, Detection Engineering: Deploy or tune detection rules for Oracle EBS exploitation indicators, specifically abnormal REST/SOAP API calls, unusual batch job execution, and outbound data transfers to non-baseline destinations.
6. Step 6, Stakeholder Notification: If Oracle EBS systems contain employee PII or organizational data, notify legal and HR. Evaluate state breach notification obligations if employee data exposure is confirmed.
7. Step 7, Long-Term Controls: Enforce network segmentation for Oracle EBS. Implement privileged access management (PAM) controls, multi-factor authentication on EBS accounts, and a formal patch cadence aligned to Oracle CPU release cycles.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate to external IR firm or managed security provider if: (a) evidence of active data exfiltration in past 30 days is found, (b) forensic timeline shows insider access (privileged account misuse by legitimate user), or (c) data inventory scope exceeds 100K+ employee records or includes regulated data (HIPAA, PCI-DSS, GDPR-regulated individuals).
Recovery Notes	Post-containment recovery: (1) Force credential rotation for all EBS users with access to HR/payroll data; stage new passwords securely via PAM or encrypted channel. (2) Conduct forensic carve of database transaction logs (undo tablespace, redo logs, archive logs) to reconstruct exact data accessed during compromise window — this informs notification scope and regulatory disclosure. (3) Implement continuous monitoring for 180 days post-recovery: weekly user account audits, daily log review for repeat exploitation patterns, monthly patch compliance checks aligned to Oracle CPU calendar.

<table>
<tr><td><b>Forensic Artifacts</b></td><td>Oracle dba_audit_trail (comprehensive DML/DDL audit log; query for past 120 days with focus on SELECT, EXTRACT, and GRANT actions) | Oracle FND_LOG and FND_AUDIT_AUDIT (EBS application-level activity log; filter on user creation, responsibility assignment, form access) | Oracle alert logs ($ORACLE_BASE/diag/rdbms/*/trace/alert_*.log; errors, exceptions, security events during compromise window) | Firewall/proxy logs and netflow records (outbound TCP connections from EBS servers; extract destination IPs, ports, byte counts, timestamps) | Web server access logs (/var/log/apache2/access.log or IIS logs for EBS Forms/Reports; URI paths, response codes, byte counts; detect exfil-sized transfers to external IP)</td></tr>
</table>

Per-Action IR Details

Step 1 — Inventory: Identify all Oracle EBS deployments in your environment, including version, patch level, and network exposure. Prioritize internet-facing or DMZ-adjacent instances.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2.1 (Preparation phase — tools and resources)

Controls: NIST 800-53 CM-8 (Information System Component Inventory), NIST 800-53 RA-3 (Risk Assessment), CIS 1.1 (Hardware Inventory)

Compensating: Query Oracle EBS installation registry: `SELECT DISTINCT instance_name, version FROM v$instance;` via SQL*Plus. Cross-reference with ps/tasklist for running processes (oracle.exe, oracleservername). Use nmap or netstat: `netstat -ano | findstr 1521` (default Oracle listener port) to map network exposure. Document in spreadsheet with instance name, version, listening ports, and DMZ/internet accessibility flagged.

Evidence: Capture output of `SELECT * FROM v$version;`, `SELECT * FROM dba_registry;` (patch registry), and full network socket state (`netstat -ano` or `ss -tlnp` on Linux). Screenshot firewall rules allowing inbound 1521, 8000-8100 (Oracle Forms/Reports). Preserve any change management records documenting EBS version/patch dates.

Step 2 — Patch Review: Cross-reference your Oracle EBS patch level against Oracle's January and April 2025 Critical Patch Update advisories. Apply any outstanding patches, with priority on authentication and access control fixes.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2.1 (Preparation — patch management); NIST 800-53 SI-2 (Flaw Remediation)

Controls: NIST 800-53 SI-2 (Flaw Remediation), NIST 800-53 CM-3 (Configuration Change Control), CIS 2.4 (Patch Management)

Compensating: Download Oracle EBS Critical Patch Update advisories (January and April 2025) from My Oracle Support (MOS). Manually compare your EBS version against each advisory's affected versions list. Document missing patches in a spreadsheet with CVE, severity, and release date. For air-gapped systems, request patches via secure transfer and stage in isolated repository; apply via `adpatch` command with staged patches. Maintain version control of applied patches in change log.

Evidence: Screenshot or text export of Oracle MOS patch applicability report for your EBS version. Record output of `SELECT * FROM dba_registry_sqlpatch;` (applied SQL patches) and file system timestamps of EBS installation directory (to verify patch application dates). Preserve pre-patch backup manifests and post-patch validation reports (adctrl logs).

Step 3 — Access Audit: Review Oracle EBS user accounts for signs of account misuse or creation of unauthorized accounts (T1078). Disable or rotate credentials for privileged accounts with no recent legitimate activity.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2.2 (Detection and Analysis — unusual account activity)

Controls: NIST 800-53 AC-2 (Account Management), NIST 800-53 AC-3 (Access Enforcement), NIST 800-53 AU-2 (Audit Events), CIS 5.2 (User Access Rights Reviews)

Compensating: Query Oracle EBS user table: `SELECT user_id, user_name, created_by, creation_date, last_update_date FROM fnd_user WHERE creation_date >= TRUNC(SYSDATE - 90) ORDER BY creation_date DESC;` to find accounts created in past 90 days. Cross-reference against change management approvals. For privileged accounts (SYSADMIN, GL_ADMINISTRATOR), query: `SELECT fu.user_name, fu.last_logon_date FROM fnd_user fu WHERE fu.user_id IN (SELECT user_id FROM fnd_user_resp_groups WHERE responsibility_id IN (SELECT responsibility_id FROM fnd_responsibility WHERE responsibility_name LIKE '%SYSTEM%')) ORDER BY fu.last_logon_date;` to identify inactive privileged accounts. Export to CSV and mark for credential rotation.

Evidence: Full export of fnd_user and fnd_user_resp_groups tables (with dates and audit columns). Capture last_logon_date and last_update_date for all privileged accounts. Pull Oracle EBS audit logs (FND_AUDIT_AUDIT, FND_LOG tables) filtered on user creation and privilege assignment events for past 120 days. Query `SELECT * FROM dba_audit_trail WHERE action_name IN ('CREATE USER', 'DROP USER', 'GRANT ROLE') AND TRUNC(timestamp) >= TRUNC(SYSDATE - 120);`

Step 4 — Log Review: Pull Oracle EBS application logs, database audit logs, and network egress logs for the past 90 days. Look for anomalous data access patterns against HR, payroll, and organizational data repositories (T1213) and large or unusual outbound transfers (T1567).

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2.3 (Detection and Analysis — log analysis)

Controls: NIST 800-53 AU-4 (Audit Log Storage), NIST 800-53 SI-4 (Information System Monitoring), NIST 800-53 SC-7 (Boundary Protection), CIS 6.2 (Activate Audit Logging)

Compensating: Enable database auditing (if not already on): `AUDIT ALL BY ;` then query `SELECT * FROM dba_audit_trail WHERE USERNAME='' AND TRUNC(TIMESTAMP) >= TRUNC(SYSDATE - 90) AND (ACTION_NAME LIKE '%SELECT%' OR ACTION_NAME LIKE '%EXTRACT%') AND (OBJ_NAME LIKE '%HR%' OR OBJ_NAME LIKE '%PAY%' OR OBJ_NAME LIKE '%EMP%');`. Export FND_LOG records: `SELECT * FROM fnd_log WHERE log_level >= 3 AND creation_date >= SYSDATE - 90 AND (message_text LIKE '%DOWNLOAD%' OR message_text LIKE '%EXPORT%');`. Pull firewall/proxy logs (netflow, firewall permit logs) for outbound connections from EBS servers to non-whitelisted destinations — look for large data transfers (TCP window size, byte counts) to IP ranges not in baseline. Use grep/awk to extract destination IPs with byte counts > 100MB in 90-day window.

Evidence: Export full dba_audit_trail for past 120 days to CSV. Capture FND_LOG, FND_AUDIT_AUDIT tables filtered to user, object, and date ranges. Pull firewall permit logs for EBS server source IPs (netflow records preferred; parse with nfdump: `nfdump -r -R 'src ip ' | awk '{if ($bytes > 104857600) print}' | sort -k $bytes -n`). Screenshot proxy/DLP logs if available (Symantec, Forcepoint, etc.). Archive database alert logs ($ORACLE_BASE/diag/rdbms/orcl/orcl/trace/alert_orcl.log) for error/exception events during suspected compromise window.

Step 5 — Detection Engineering: Deploy or tune detection rules for Oracle EBS exploitation indicators — specifically, abnormal REST/SOAP API calls, unusual batch job execution, and outbound data transfers to non-baseline destinations.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.3 (Containment); NIST 800-53 SI-4 (Information System Monitoring)

Controls: NIST 800-53 SI-4 (Information System Monitoring), NIST 800-53 SC-7 (Boundary Protection), CIS 7.1 (Deploy a Host-based Intrusion Detection Tool)

Compensating: Create detection rules in free/open-source tools (Suricata, Zeek, osquery) targeting: (1) REST/SOAP API abuse — monitor /fnd_sso/oauth2/rest endpoint access; flag GET/POST requests with large response sizes (>10MB) or multiple rapid sequential calls (>50 in 5min) from single source IP; (2) batch job anomalies — query FND_CONCURRENT_REQUESTS for jobs submitted outside normal business hours (22:00-06:00) or submitted by unprivileged accounts; (3) egress baseline violation — capture normal egress IP ranges/ports via 30-day whitelist, then alert on connections outside whitelist. Use osquery: `SELECT * FROM process_open_sockets WHERE remote_port NOT IN (443, 80, 22) AND remote_address NOT IN () AND time > ;`

Evidence: Document baseline normal API call patterns (response sizes, frequency, users, times) by querying EBS access logs for 30-day clean period. Capture sample REST/SOAP requests (with headers, parameters redacted for

PII). Export FND_CONCURRENT_REQUESTS for past 180 days to identify normal batch job submission windows and users. Baseline network egress with tcpdump/Wireshark: `tcpdump -i eth0 src and (dst port 443 or dst port 80 or dst port 22) -w baseline.pcap` over 7-day clean period, then parse with tshark to extract destination IPs, ports, protocols.

Step 6 — Stakeholder Notification: If Oracle EBS systems contain employee PII or organizational data, notify legal and HR. Evaluate state breach notification obligations if employee data exposure is confirmed.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §3.4.1 (Post-Incident — notification); NIST 800-53 IR-6 (Incident Reporting)

Controls: NIST 800-53 IR-6 (Incident Reporting), NIST 800-53 IR-1 (Incident Response Policy), CIS 6.5 (Restrict Administrator Privileges)

Compensating: Establish incident notification timeline per NIST 800-61r3 §3.4.1: Legal (within 24h for potential breach), HR (within 48h if employee PII affected), Privacy Officer (within 72h). Create brief factual summary: affected systems, data categories accessed (HR, payroll, employee records), date range of exposure, confirmation status. Consult breach notification law database (e.g., SANS Breach Notification State Law Chart) to determine notification timelines by state where employees reside; most states require notification within 30-60 days. Document all notifications in incident log with timestamps and recipients.

Evidence: Preserve incident summary email and stakeholder notification records (to/from/date). Maintain log of who accessed incident data (principle of least privilege). Document data exposure scope: count of affected employee records, data elements exposed (SSN, date of birth, salary, address), systems involved, confirmation method (logs, witness account, etc.).

Step 7 — Long-Term Controls: Enforce network segmentation for Oracle EBS. Implement privileged access management (PAM) controls, multi-factor authentication on EBS accounts, and a formal patch cadence aligned to Oracle CPU release cycles.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.4.2 (Post-Incident — recovery); NIST 800-53 SC-7 (Boundary Protection), AC-2 (Account Management)

Controls: NIST 800-53 SC-7 (Boundary Protection), NIST 800-53 AC-2 (Account Management), NIST 800-53 IA-4 (Identifier Management), NIST 800-53 SI-2 (Flaw Remediation), CIS 6.3 (MFA for all Remote Access Users)

Compensating: Network segmentation: create dedicated VLAN for Oracle EBS (10.x.x.0/24), restrict inbound to admin jump box via ACL; configure firewall to deny EBS-to-internet traffic except pre-approved egress (patch server, monitoring). PAM without enterprise tool: implement file-based privilege escalation via sudo on Linux; configure /etc/sudoers with time-based and command-based restrictions (e.g., `%dba ALL=(root) 09:00-17:00 /usr/local/bin/adpatch`). MFA without vendor solution: use Google Authenticator or FreeOTP (TOTP-based) on EBS login screen; integrate with PAM solution (CyberArk open-source alternatives: HashiCorp Vault, BeyondTrust Privileged Remote Access). Patch cadence: subscribe to Oracle Critical Patch Update (CPU) calendar (Jan, Apr, Jul, Oct); stage patches 2 weeks post-release in test environment, deploy to prod within 30 days for critical vulnerabilities.

Evidence: Document network segmentation design (firewall rules, VLAN configuration, IP ranges, ACLs). Screenshot PAM tool configuration (sudo rules, command restrictions, session logging). Preserve MFA enrollment records and TOTP seed backups (encrypted). Create and version-control patch deployment schedule document (quarterly calendar aligned to Oracle CPU dates, responsibility assignments, rollback procedures).

Detection Guidance

No confirmed IOCs (IPs, domains, hashes) have been publicly released for this campaign as of the analysis date. Detection should focus on behavioral indicators. In Oracle EBS application and database audit logs, look for: bulk SELECT or export operations against HR_ALL_PEOPLE_F, PER_ALL_ASSIGNMENTS_F, or equivalent employee data tables outside of scheduled batch windows; logins from unfamiliar source IPs or geographic locations to EBS application accounts; creation or modification of EBS user accounts or responsibility assignments not tied to a change request; Oracle concurrent requests invoking data export programs (e.g., HRMS extracts) outside normal scheduling. At the network layer, look for sustained or high-volume outbound transfers from EBS application or database servers to external destinations, particularly to cloud storage endpoints consistent with T1567 (Exfiltration Over Web Service). For endpoint and OS-level telemetry on EBS application servers, look for new scheduled tasks, cron jobs, or services not present in baseline configuration. If a SIEM is in use, correlate EBS login events against user activity baselines and flag deviations exceeding two standard deviations in data volume or access frequency. MITRE ATT&CK data source references: Application Log (T1213), Network Traffic (T1567), Logon Session (T1078), Application Log / Web Application Firewall (T1190).

Indicators of Compromise

Type	Value	Context	Confidence
NOTE	`No confirmed IOCs available`	No IP addresses, domains, file hashes, or URLs attributable to this campaign have been publicly released as of the analysis date. IOC field will be updated if indicators are published by Oracle, MSG, or a vetted threat intelligence source.	LOW

Framework Mappings

MITRE-ATTACK

- **T1567** — Exfiltration Over Web Service
- **T1078** — Valid Accounts
- **T1190** — Exploit Public-Facing Application
- **T1213** — Data from Information Repositories

NIST-800-53R5

- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **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-3** — Access Enforcement

OWASP-TOP10-2021

- **A01:2021** — Broken Access Control

CIS-V8

- **6.1**
- **6.2**

SOC2-TSC

- **CC6.1** — The entity implements logical access security software, infrastructure, and architectures over protected information assets
- **CC7.4** — Responds to identified security incidents

HIPAA-SECURITY

- **164.312(a)(1)** — Access Control
- **164.308(a)(6)(ii)** — Response and Reporting

ISO-27001-2022

- **A.5.34** — Privacy and protection of personal information

NIST-CSF-2

- **RS.CO-03** — Recovery activities and progress communicated

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1567	Exfiltration Over Web Service	Exfiltration
T1078	Valid Accounts	Defense-Evasion
T1190	Exploit Public-Facing Application	Initial-Access
T1213	Data from Information Repositories	Collection

Sources

Source	URL	Tier
	https://www.securityweek.com/madison-square-garden-data-breach-conf...	T3
Madison Data Breach Confirmed After Hacker Attack - CertPro	https://certpro.com/madison-data-breach-confirmed/	T3
The Madison Square Garden Entertainment Data Breach	https://www.forthepeople.com/blog/madison-square-garden-entertainme...	T3

Source	URL	Tier
Oracle EBS 2025 campaign impacts Madison Square Garden ...	https://securityaffairs.com/188814/cyber-crime/oracle-ebs-2025-camp...	T3
Madison Square Garden Confirms Data Breach Linked to Oracle ...	https://www.reddit.com/r/secithubcommunity/comments/1rmf7cj/madison...	T3

DISCLAIMER

This intelligence report is produced by Tech Jacks Solutions Security Command Center (SCC) for informational purposes only. It does not constitute professional security advice, legal counsel, or an incident response engagement. The information herein is derived from publicly available sources and AI-assisted analysis; while every effort is made to ensure accuracy, Tech Jacks Solutions makes no warranties regarding completeness or timeliness. Organizations should conduct their own validation and consult qualified security professionals before taking action based on this report. Tech Jacks Solutions is not liable for any damages resulting from the use of this information.

Generated 2026-03-29 18:41 UTC by TJS Security Command Center