INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-03-29 18:38 UTC

Michelin Data Breach Linked to Oracle E-Business Suite Attack Campaign

DATA BREACH | HIGH | CVSS 8.6

SCC Item ID	SCC-DBR-2026-0001
Type	Data Breach
Severity	HIGH
CVSS Base Score	8.6
Affected Products	Oracle E-Business Suite (EBS); Michelin corporate environment — specific versions not publicly confirmed
Published	1 day ago

Executive Summary

Michelin has confirmed a data breach tied to an active attack campaign targeting Oracle E-Business Suite (EBS), with approximately 300GB of data reported exfiltrated. Oracle EBS is a widely deployed ERP platform handling HR, finance, and supply chain data, making successful exploitation high-impact for any affected organization. Organizations running Oracle EBS should treat this as an active threat requiring immediate inventory and control validation, regardless of whether Michelin-specific details apply to their environment.

Technical Analysis

The breach is attributed to an attack campaign exploiting vulnerabilities in Oracle E-Business Suite (EBS). The specific CVEs leveraged have not been publicly confirmed in open-source reporting as of this analysis. The item data references a CVSS base score of 8.6, the source of that score is not confirmed against a specific CVE in available reporting and should be treated as approximate context, not authoritative. Associated weaknesses include CWE-89 (SQL Injection), CWE-284 (Improper Access Control), and CWE-306 (Missing Authentication for Critical Function). MITRE ATT&CK techniques mapped to this campaign: T1190 (Exploit Public-Facing Application) as the likely initial access vector; T1078 (Valid Accounts) suggesting possible credential abuse or session hijacking post-exploitation; T1213 (Data from Information Repositories) consistent with ERP data exfiltration; T1041 (Exfiltration Over C2 Channel) for the reported 300GB data exfiltration. Specific Oracle EBS versions affected have not been publicly confirmed. No CISA KEV entry or confirmed EPSS scoring is available for the specific vulnerability as of this analysis. Threat actor attribution is unconfirmed. Source quality for this item is limited, primary sourcing is SecurityWeek (T3); no vendor advisory or CISA alert has been identified in available open-source reporting.

Action Checklist

1. Step 1, Immediate: Inventory all Oracle EBS instances in your environment, including version numbers, internet-facing exposure, and authentication configurations. Prioritize externally accessible instances.
2. Step 2, Immediate: Review Oracle EBS patch levels against Oracle's most recent Critical Patch Update (CPU). Oracle publishes CPUs quarterly; ensure no outstanding patches for authentication, access control, or SQL injection categories are unapplied.
3. Step 3, Detection: Query web application and EBS application logs for anomalous authentication events, unexpected API calls, large data queries against HR, finance, or supply chain modules, and unusual outbound data transfers. See detection guidance below.
4. Step 4, Assessment: Confirm whether Oracle EBS instances are directly internet-facing or accessible via VPN only. Restrict direct internet exposure if not operationally required; enforce network segmentation between EBS and other enterprise systems.
5. Step 5, Communication: If Oracle EBS is deployed in your environment, brief your CISO and relevant stakeholders on the campaign. If your organization processes personal data through EBS (HR, payroll), assess whether breach notification obligations apply under GDPR, CCPA, or applicable regulation, this assessment requires legal review.
6. Step 6, Long-term: Review Oracle EBS authentication controls against CIS Benchmarks for Oracle and NIST SP 800-53 AC and IA control families. Evaluate whether privileged access to EBS is monitored via a SIEM or UEBA solution capable of detecting anomalous ERP query behavior.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate to external IR firm immediately if: (1) forensic evidence shows data exfiltration occurred within your environment, (2) EBS authentication controls review identifies compromised privileged accounts, or (3) legal review determines breach notification obligations and your organization lacks breach notification playbook experience.
Recovery Notes	Post-containment recovery: (1) reapply all Oracle Critical Patch Updates and test in staging before production deployment; (2) force password reset for all EBS users, especially privileged accounts, and require MFA re-enrollment; (3) conduct forensic analysis of database audit trails and application logs to determine if data exfiltration occurred and quantify the scope (requires full audit trail preservation from Step 3); (4) implement continuous monitoring of EBS authentication events and SQL queries against sensitive modules (HR, Finance) using either SIEM ingestion or daily manual log review if SIEM unavailable; (5) document all control improvements in your security control matrix (map to NIST 800-53 AC/IA families) and schedule re-assessment in 90 days.
Forensic Artifacts	Oracle EBS database audit trail (dba_audit_trail table, exported to immutable CSV with MD5 hash) | Application tier logs ($ORACLE_HOME/appsutil/log/, FND concurrent request logs) \| Web/proxy server access logs (Apache access.log, IIS logs, proxy/firewall logs with HTTP headers and source IPs) \| Database listener logs ($ORACLE_HOME/network/log/listener.log, SQL trace files if enabled) | OS authentication logs (/var/log/auth.log, /var/log/secure, Windows Event Log 4624 Logon Success and 4625 Logon Failure)

Per-Action IR Details

Step 1, Immediate: Inventory all Oracle EBS instances in your environment, including version numbers, internet-facing exposure, and authentication configurations. Prioritize externally accessible instances.

NIST Phase: Preparation

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

Controls: NIST 800-53 CM-2 (Baseline Configuration), NIST 800-53 CA-7 (Continuous Monitoring), CIS v8 Control 1 (Inventory and Control of Enterprise Assets)

Compensating: Use Oracle EBS native SQL query to enumerate instances: select * from fnd_product_installations; document via spreadsheet with columns: hostname, version, listener port, public IP/private IP, authentication method (LDAP/local), last patch date. For internet-facing detection without vulnerability scanner, query firewall ACLs and network diagrams; cross-reference with DNS (nslookup) and curl/telnet on port 8000 (default EBS web tier) from external network segment.

Evidence: Before inventory: capture current firewall rules (iptables -L -n or Windows Firewall export), routing table (route -n or route print), DNS resolution logs (/var/log/named or Windows DNS Server logs Event ID 4741), and network interface configuration (ifconfig -a or ipconfig /all). Baseline these to detect subsequent changes.

Step 2, Immediate: Review Oracle EBS patch levels against Oracle's most recent Critical Patch Update (CPU). Oracle publishes CPUs quarterly; ensure no outstanding patches for authentication, access control, or SQL injection categories are unapplied.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2.1 (Preparation: patching and vulnerability management)

Controls: NIST 800-53 SI-2 (Flaw Remediation), NIST 800-53 SI-3 (Malicious Code Protection), CIS v8 Control 3 (Address Unauthorized Software), CIS Oracle 2.3.1 (Apply Latest Security Patches)

Compensating: Query EBS patch history via SQL: select * from ad_bugs where bug_fixed_in_version is not null order by creation_date desc; compare against Oracle CPU advisory list (publicly available at oracle.com/security-alerts, requires free Oracle account). For air-gapped environments, download CPU readme from Oracle Support on connected system, transfer via USB, and manually verify patch numbers in your EBS version. Document patch application dates in change control log with MD5/SHA256 hash of patch binary for integrity validation.

Evidence: Capture EBS version output (select fnd_release.major_version from dual), all applied patch IDs (select bug_number from ad_bugs where bug_number is not null), patch installation log timestamps ($ORACLE_HOME/appsutil/log/), and system.sql query results showing current applied patches. Archive these in read-only format before any patching activity begins.

Step 3, Detection: Query web application and EBS application logs for anomalous authentication events, unexpected API calls, large data queries against HR, finance, or supply chain modules, and unusual outbound data transfers. See detection guidance below.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 (Detection and Analysis)

Controls: NIST 800-53 AU-2 (Audit Events), NIST 800-53 AU-12 (Audit Record Generation), NIST 800-53 SI-4 (Information System Monitoring), CIS v8 Control 8 (Audit Log Management)

Compensating: Without SIEM: manually query EBS logs in $ORACLE_HOME/forms/log/ and $ORACLE_HOME/conc/log/ for failed login attempts (grep -i 'invalid.*user\|fnd_user.validate_login' *.log). Check concurrent manager logs for unexpected module access (grep -i 'hr\|payroll\|finance\|supply' *.log). Query database audit trail: select username, timestamp, sqltext from dba_audit_trail where obj_name in ('PER_ALL_PEOPLE_F','GL_JE_HEADERS') and timestamp > trunc(sysdate)-30 order by timestamp desc. For outbound transfers, check netstat -tuln during business hours and compare against baseline; capture with tcpdump -i any -w ebs_traffic.pcap 'not (port 22 or port 53)' for 1-hour samples.

Evidence: Preserve EBS application logs ($ORACLE_HOME/appsutil/log/, $ORACLE_INSTANCE/logs/), database audit logs (enable if not already: alter system set audit_trail=DB scope=spfile; restart database), Apache/web server access logs (/var/log/apache2/access.log or IIS logs in %SystemRoot%\System32\LogFiles), and concurrent request logs (Query fnd_concurrent_requests table for requests with large row counts or long run times). Capture firewall

egress logs and proxy logs if applicable. Hash all logs before analysis to preserve chain of custody.

Step 4, Assessment: Confirm whether Oracle EBS instances are directly internet-facing or accessible via VPN only. Restrict direct internet exposure if not operationally required; enforce network segmentation between EBS and other enterprise systems.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 (Containment)

Controls: NIST 800-53 AC-3 (Access Enforcement), NIST 800-53 SC-7 (Boundary Protection), NIST 800-53 AC-4 (Information Flow Enforcement), CIS v8 Control 13 (Network Architecture)

Compensating: Map network topology manually: run traceroute from external network to EBS hostname; if reachable directly, EBS is internet-facing. Document with: nmap -sV -p 8000,8443,1521 from external host (does NOT require full nmap installation; can use curl -v https://:8443 to test connectivity). Implement UFW (ufw allow from to any port 8000) or Windows Firewall rule (netsh advfirewall firewall add rule name="EBS_VPN_Only" dir=in action=block remoteip=0.0.0.0/0 protocol=tcp localport=8000). Test with: curl https://:8000 (should timeout after implementing rule). Document baseline rules before change.

Evidence: Capture baseline firewall configuration (iptables-save > baseline_fw.txt or export firewall rules via Powershell: Get-NetFirewallRule -Direction Inbound > baseline_fw.csv), routing tables (ip route show > baseline_routes.txt), and network interface bindings (netstat -tuln > baseline_listeners.txt). Create timestamp-stamped copies on write-protected storage; these establish the pre-incident state for forensic comparison.

Step 5, Communication: If Oracle EBS is deployed in your environment, brief your CISO and relevant stakeholders on the campaign. If your organization processes personal data through EBS (HR, payroll), assess whether breach notification obligations apply under GDPR, CCPA, or applicable regulation, this assessment requires legal review.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2.3 (Communication and Information Sharing)

Controls: NIST 800-53 IR-4 (Incident Handling), NIST 800-53 SA-9 (External Information System Services), CIS v8 Control 19 (Incident Response Management)

Compensating: Without legal team on-call: document data inventory in EBS (query data dictionary to identify PII tables: select owner, table_name from dba_tables where table_name like '%PERSON%' or '%PAYROLL%' or '%EMPLOYEE%'; do not extract data, only count rows and note presence). Flag for legal review in writing with timestamp. Prepare internal incident report template documenting: affected EBS instance(s), affected modules (HR/Finance/Supply Chain), data types at risk (personal data yes/no), number of records affected (if known). Escalate to CISO with this summary and regulatory deadline calendar (GDPR: 72 hours, CCPA: without unreasonable delay per intent). Record escalation in writing.

Evidence: Preserve all communications (email, Slack, meeting notes) regarding the threat discovery and stakeholder briefing. Document data classification tags applied to EBS in your asset management system. Capture screenshots of EBS audit logs showing data access (before any deletion or retention policy purge). Maintain decision log showing legal review date and determination.

Step 6, Long-term: Review Oracle EBS authentication controls against CIS Benchmarks for Oracle and NIST SP 800-53 AC and IA control families. Evaluate whether privileged access to EBS is monitored via a SIEM or UEBA solution capable of detecting anomalous ERP query behavior.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.4 (Eradication and Recovery); §4 (Post-Incident Activities)

Controls: NIST 800-53 AC-2 (Account Management), NIST 800-53 IA-2 (Authentication), NIST 800-53 IA-4 (Identifier Management), NIST 800-53 IA-5 (Authenticator Management), NIST 800-53 AU-12 (Audit Record Generation), CIS Oracle 2.1 (Ensure Default Accounts Are Locked and Passwords Changed), CIS Oracle 2.2 (Ensure User Accounts are Locked with Password Expiration Enabled)

Compensating: Audit authentication manually: query select username, account_status, expiry_date from dba_users where account_status != 'EXPIRED' order by created; disable default accounts (SCOTT, SYS, SYSTEM if unused). Implement MFA via OS-level authentication: enforce PAM (Pluggable Authentication Modules) for SSH (edit /etc/pam.d/sshd to require TOTP or hardware key). Query privileged EBS user activity: select username, timestamp, action_name, obj_name from dba_audit_trail where username in (select name from fnd_user where employee_id is null) and sqltext like '%SELECT%' order by timestamp desc. Export to CSV weekly and manually review for anomalies (unusual times, repeated failed auth, large data extracts). Document review findings in change control log. Establish baseline of 'normal' privileged queries for comparison.

Evidence: Capture EBS user account audit trail (select * from dba_users and fnd_user tables exported to timestamped CSV). Document current authentication method (LDAP, local DB, OID). Archive baseline privileged query logs for the 30 days prior to this incident (full SQL text, not summaries). Create and sign-off on authentication control policy (password complexity, expiration, MFA requirement, account lockout thresholds) for auditor reference. Preserve evidence of SIEM/UEBA configuration capability assessment (tool comparison matrix if no tool exists).

Detection Guidance

No confirmed IOCs (IPs, domains, hashes) have been publicly released for this campaign as of this analysis. Detection should focus on behavioral indicators within Oracle EBS and surrounding infrastructure. Key areas to investigate: (1) Authentication anomalies, review Oracle EBS FND_LOGINS and WF_LOCAL_ROLES audit tables for accounts authenticating outside normal hours, from unexpected source IPs, or with elevated privilege usage not matching role assignments; (2) SQL Injection indicators, review Oracle database audit logs (V$SQL, AUDIT_TRAIL) for unusual query patterns targeting HR, payroll, or financial tables, particularly queries with UNION, OR 1=1 patterns, or unexpected procedural calls; (3) Data staging and exfiltration, look for large SELECT operations against sensitive EBS modules (PER_ALL_PEOPLE_F, AP_INVOICES_ALL, GL_JE_LINES) by non-scheduled processes, followed by outbound network connections to unfamiliar external IPs; (4) Valid account abuse, correlate EBS authentication events against directory services (Active Directory, LDAP) to identify accounts authenticating to EBS that have not been used recently or that are accessing modules outside their normal job function; (5) Network, monitor for sustained outbound data transfers (volume and duration anomalies) from EBS application servers to external destinations. Specific SIEM query logic will depend on your EBS version and logging configuration. Oracle EBS audit logging must be enabled and forwarded to your SIEM for these detections to function, verify this as a prerequisite.

Indicators of Compromise

Type	Value	Context	Confidence
URL	`No confirmed IOCs available`	No specific IPs, domains, hashes, or URLs have been publicly attributed to this campaign in available open-source reporting as of this analysis. This field will be updated if IOCs are released by Oracle, CISA, or a credible threat intelligence provider.	LOW

Framework Mappings

MITRE-ATTACK

- **T1213** — Data from Information Repositories
- **T1078** — Valid Accounts
- **T1190** — Exploit Public-Facing Application
- **T1041** — Exfiltration Over C2 Channel

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
- **CA-7** — Continuous Monitoring
- **SI-4** — System Monitoring
- **SR-2** — Supply Chain Risk Management Plan

HIPAA-SECURITY

- **164.308(a)(6)(ii)** — Response and Reporting

SOC2-TSC

- **CC7.4** — Responds to identified security incidents
- **CC9.2** — Manages risks associated with vendors and business partners

ISO-27001-2022

- **A.5.34** — Privacy and protection of personal information
- **A.5.21** — Managing information security in the ICT supply chain

NIST-CSF-2

- **RS.CO-03** — Recovery activities and progress communicated
- **GV.SC-01** — Cybersecurity supply chain risk management program

CIS-V8

- **15.1** — Establish and Maintain an Inventory of Service Providers

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1213	Data from Information Repositories	Collection

Technique ID	Technique Name	Tactic
T1078	Valid Accounts	Defense-Evasion
T1190	Exploit Public-Facing Application	Initial-Access
T1041	Exfiltration Over C2 Channel	Exfiltration

Sources

Source	URL	Tier
SecurityWeek	https://www.securityweek.com/michelin-confirms-data-breach-linked-t...	T3
Michelin Faces Data Breach Linked to Oracle EBS Exploit - Reddit	https://www.reddit.com/r/pwnhub/comments/1rqsjoe/michelin_faces_dat...	T3
Michelin Confirms Data Breach Linked to Oracle EBS Attack - LinkedIn	https://www.linkedin.com/posts/cyber-news-live_michelin-confirms-da...	T3
Michelin Confirms Data Breach Linked to Oracle EBS Attack - X	https://x.com/SecurityWeek/status/2031694227256565929	T3
InvulnerNews on Instagram: "Michelin's 300GB Data Breach ...	https://www.instagram.com/p/DVviLE8jhVU/	T3

Generated 2026-03-29 18:38 UTC by TJS Security Command Center