INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-03 06:53 UTC

CISA Confirms Active Exploitation of Oracle WebLogic CVE-2024-21182, Unauthenticated Takeover Risk Demands Immediate Patching

CVE VULNERABILITY | **CRITICAL** | CVSS 9.5

SCC Item ID	SCC-CVE-2026-0258
Type	CVE Vulnerability
CVE ID	CVE-2024-21182
Severity	CRITICAL
CVSS Base Score	9.5
EPSS Score	0.8965 (100th percentile)
Affected Products	Oracle WebLogic Server (specific affected versions not confirmed from available sources; consult Oracle Critical Patch Update advisory for version scope)
Published	2026-06-02T14:14:42
Discovery Source	Rss

Executive Summary

CISA confirmed active exploitation of CVE-2024-21182, a critical vulnerability in Oracle WebLogic Server that allows unauthenticated attackers to fully compromise affected systems over the network. Organizations running WebLogic in financial services, government, and healthcare face immediate risk of server takeover, data exfiltration, and ransomware deployment. With a CVSS score of 9.5 and an EPSS score placing it in the 99th percentile for exploitation probability, this requires emergency patch action, not scheduled maintenance.

Technical Analysis

CVE-2024-21182 is a critical-severity flaw in Oracle WebLogic Server, classified under CWE-284 (Improper Access Control) and CWE-306 (Missing Authentication for Critical Function). The vulnerability exposes critical server functionality without requiring authentication, enabling a remote, unauthenticated attacker with network access to achieve full server compromise. CVSS base score is 9.5. EPSS score is 0.897 (99.58th percentile), indicating very high near-term exploitation probability. CISA confirmed active exploitation and added this CVE to the Known Exploited Vulnerabilities catalog in June 2026. The CVE was originally assigned in 2024, with confirmed in-the-wild exploitation detected in 2026, a two-year gap consistent with deferred exploitation timelines observed in enterprise infrastructure vulnerabilities. Applicable MITRE ATT&CK techniques include

T1190 (Exploit Public-Facing Application), T1505.003 (Server Software Component: Web Shell), T1210 (Exploitation of Remote Services), T1059 (Command and Scripting Interpreter), and T1133 (External Remote Services). Initial exploitation does not require valid accounts; T1078 may apply post-compromise for lateral movement and persistence. Specific affected version ranges are not confirmed from available sources; consult the Oracle Critical Patch Update advisory directly for authoritative version scope. Patch status: Oracle has issued a fix; refer to the Oracle CPU advisory for the applicable patch ID and version upgrade path.

Action Checklist

1. Step 1: Containment, Identify all Oracle WebLogic Server instances in your environment using your asset inventory (NIST CM-8, CIS 1.1). Immediately restrict inbound network access to WebLogic admin ports (default 7001, 7002, 9002) at the perimeter firewall and host-based firewall (CIS 4.4, CIS 4.5, NIST AC-4) for any instance not yet patched. If internet-facing WebLogic instances exist, consider emergency isolation or WAF rule deployment blocking unauthenticated requests to affected endpoints pending patch.
2. Step 2: Detection, Query SIEM and endpoint telemetry for anomalous activity against WebLogic servers: (a) unexpected outbound connections from WebLogic process (wls process) to external IPs; (b) new files written to WebLogic deployment directories (System File Analysis, CIS 8.4); (c) unusual child processes spawned by WebLogic JVM (cmd.exe, /bin/bash, powershell.exe); (d) review WebLogic server access logs for unauthenticated requests to T3/T3S protocol endpoints and IIOP listeners; (e) check for new or modified .war/.ear files in autodeploy directories (File Magic Byte Verification, CIS 2.5). Enable and collect audit logs per NIST AU-2 and CIS 8.2 if not already active.
3. Step 3: Eradication, Apply Oracle's Critical Patch Update fix for CVE-2024-21182 to all affected WebLogic instances. Consult Oracle's Critical Patch Update (CPU) advisory page at https://www.oracle.com/security-alerts/ to locate the appropriate monthly CPU (search by CVE-2024-21182 within the advisory) to confirm the exact patch ID and eligible version upgrade path for your deployment. After patching, rotate all service account credentials and API keys associated with WebLogic (NIST AC-2, CIS 1.2). Remove or disable the T3 and IIOP protocols if not operationally required, as these are common exploitation entry points for WebLogic vulnerabilities.
4. Step 4: Recovery, After patching, verify WebLogic server version and patch level through the Oracle inventory tool. Conduct a targeted review of WebLogic deployment directories for unauthorized files or web shells (T1505.003 indicator; system file analysis). Validate that admin console access requires authentication and is restricted to authorized management networks (NIST AC-3, AC-17). Monitor WebLogic process behavior for 72 hours post-patch using endpoint detection telemetry. Re-enable any isolated services in a controlled, monitored sequence.
5. Step 5: Post-Incident, Review your patch management SLA against the two-year gap between CVE assignment (2024) and confirmed exploitation (2026) to determine if deferred patching contributed to exposure (CIS 7.1, CIS 7.2, NIST SI-4). Assess whether WebLogic instances are inventoried and included in your vulnerability scanning scope (CIS 1.1, CIS 7.3, CIS 7.4). Evaluate whether least-privilege network segmentation (NIST AC-6, AC-4) would have limited blast radius had exploitation occurred. Document lessons learned and update WebLogic-specific playbooks.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE

Escalation Criteria	Escalate to CISO and initiate breach notification assessment immediately if any of the following are confirmed: unauthorized files (.war, .ear, .jsp) found in WebLogic deployment or tmp directories, outbound connections from the WebLogic JVM process to external IPs detected, child processes (cmd.exe, /bin/bash, powershell.exe) spawned by java.exe with no authorized change record, or if the affected WebLogic instance hosts applications processing PII, PHI, or financial data subject to HIPAA, PCI-DSS, or state breach notification statutes.
Recovery Notes	After applying the Oracle CPU patch for CVE-2024-21182, verify patch application via OPatch lsinventory and confirm T3/IIOP are disabled or access-restricted before restoring network connectivity to ports 7001, 7002, and 9002. Conduct a file integrity sweep of all WebLogic deployment directories, autodeploy paths, and JVM temp directories for web shells (MITRE ATT&CK T1505.003) using YARA rules before returning the system to production. Maintain elevated monitoring of WebLogic process behavior, outbound network connections from the JVM, and new file creation events in deployment directories for a minimum of 72 hours post-recovery, given the active exploitation status confirmed by CISA.
Forensic Artifacts	WebLogic server logs at /servers//logs/.log — filter for T3/T3S handshake entries and unauthenticated IIOP listener requests, which represent the CVE-2024-21182 exploitation vector over ports 7001/7002 | WebLogic autodeploy and deployment directories (/autodeploy/, /servers//tmp/_WL_user/) — unauthorized .war, .ear, or .jsp/.jspx files indicate post-exploitation payload staging or web shell installation (MITRE ATT&CK T1505.003) | Java process ancestry logs from Sysmon Event ID 1 (Windows) or auditd EXECVE syscall records (Linux) — specifically java.exe or javaw.exe spawning cmd.exe, powershell.exe, or /bin/sh, indicating successful remote code execution via the WebLogic JVM following CVE-2024-21182 exploitation | Network connection logs (Sysmon Event ID 3 or netflow/firewall logs) filtered for outbound connections originating from the java.exe/java PID to non-RFC1918 addresses — post-exploitation C2 beaconing or data exfiltration from a compromised WebLogic instance would appear here | WebLogic config.xml at /config/config.xml and JDBC datasource files at /config/jdbc/ — attackers with post-exploitation access commonly harvest these files for database credentials and connection strings stored in cleartext or weakly encrypted form

Per-Action IR Details

Step 1: Containment — Identify all Oracle WebLogic Server instances in your environment using your asset inventory (NIST CM-8, CIS 1.1). Immediately restrict inbound network access to WebLogic admin ports (default 7001, 7002, 9002) at the perimeter firewall and host-based firewall (CIS 4.4, CIS 4.5, NIST AC-4) for any instance not yet patched. If internet-facing WebLogic instances exist, consider emergency isolation or WAF rule deployment blocking unauthenticated requests to affected endpoints pending patch.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy

Controls: NIST AC-4 (Information Flow Enforcement), NIST CM-8 (System Component Inventory), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 4.5 (Implement and Manage a Firewall on End-User Devices)

Compensating: For teams without a CMDB, run: `nmap -p 7001,7002,9002 --open -oN weblogic_scan.txt` to enumerate exposed WebLogic ports across your network. Block those ports immediately using iptables: `iptables -I INPUT -p tcp --dport 7001 -j DROP` (repeat for 7002, 9002). On Windows hosts, use: `netsh advfirewall firewall add rule name='Block WLS 7001' dir=in action=block protocol=TCP localport=7001`. For WAF compensating control without budget, deploy ModSecurity with the OWASP Core Rule Set and add a custom rule blocking unauthenticated T3/IIOP handshake patterns to WebLogic-facing vhosts.

Evidence: Before blocking ports, capture a netstat snapshot to document all active inbound connections to ports 7001, 7002, and 9002: `netstat -antp | grep -E '7001|7002|9002'` (Linux) or `netstat -ano | findstr '7001'` (Windows). Export

current WebLogic server access logs from `/servers//logs/.log` and `access.log` to preserve any pre-containment T3/IIOP connection attempts. Capture firewall connection state tables before applying block rules — these may contain attacker IPs already in established state that would be lost after ACL application.

Step 2: Detection — Query SIEM and endpoint telemetry for anomalous activity against WebLogic servers: (a) unexpected outbound connections from WebLogic process (wls process) to external IPs; (b) new files written to WebLogic deployment directories (D3-SFA — System File Analysis); (c) unusual child processes spawned by WebLogic JVM (cmd.exe, /bin/bash, powershell.exe); (d) review WebLogic server access logs for unauthenticated requests to T3/T3S protocol endpoints and IIOP listeners; (e) check for new or modified .war/.ear files in autodeploy directories (D3-FMBV — File Magic Byte Verification). Enable and collect audit logs per NIST AU-2 and CIS 8.2 if not already active.

NIST Phase: Detection Analysis

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

Controls: NIST AU-2 (Event Logging), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST SI-4 (System Monitoring), CIS 8.2 (Collect Audit Logs)

Compensating: Deploy Sysmon (config: SwiftOnSecurity baseline minimum) on WebLogic Windows hosts and add ProcessCreate rules filtering for java.exe or javaw.exe as parent with cmd.exe, powershell.exe, or wscript.exe as child — these indicate JVM code execution post-exploitation of CVE-2024-21182. On Linux, use auditd with: `auditctl -a always,exit -F arch=b64 -S execve -F ppid=$(pgrep -f weblogic) -k weblogic_exec`. Monitor autodeploy directories with: `find /autodeploy -newer /tmp/baseline_timestamp -name '*.war' -o -name '*.ear'` run via cron every 5 minutes. Use osquery with: `SELECT * FROM file WHERE path LIKE '/autodeploy/%' AND type='regular' AND mtime > (strftime('%s','now') - 3600);`

Evidence: Collect WebLogic server logs at `/servers//logs/.log` and filter for T3 handshake entries and IIOP listener activity — CVE-2024-21182 exploitation will appear as unauthenticated deserialization requests over T3/T3S (port 7001/7002). Capture Java process tree snapshots: `ps auxf | grep java` (Linux) or Sysmon Event ID 1 (Process Create) with ParentImage matching java.exe. Check `/servers//tmp/_WL_user/` and autodeploy directories for .war/.ear files with creation timestamps post-exposure window. On Windows, query: `wevtutil qe Security /q:"*[System[EventID=4688] and EventData[Data[@Name='ParentProcessName'] and (Data='java.exe')]]" /f:text`.

Step 3: Eradication — Apply Oracle's Critical Patch Update fix for CVE-2024-21182 to all affected WebLogic instances. Consult the Oracle CPU advisory at https://www.oracle.com/security-alerts/ to confirm the exact patch ID and eligible version upgrade path for your deployment. After patching, rotate all service account credentials and API keys associated with WebLogic (D3-CRO — Credential Rotation, NIST AC-2). Remove or disable the T3 and IIOP protocols if not operationally required, as these are common exploitation entry points for WebLogic vulnerabilities.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST AC-2 (Account Management), NIST SI-2 (Flaw Remediation), CIS 7.3 (Perform Automated Operating System Patch Management), CIS 7.4 (Perform Automated Application Patch Management)

Compensating: If the Oracle CPU patch cannot be applied immediately, disable T3 and IIOP via WebLogic console or WLST script as a documented compensating control: in `config.xml`, set `true` and remove T3 from enabled protocols. Use WLST offline: `readDomain(''); cd('Servers/AdminServer'); set('ListenPort', 7001); writeDomain('')`. Rotate WebLogic admin account and any datasource passwords stored in `/config/jdbc/` using the WebLogic Encryption utility (`weblogic.security.Encrypt`). Document this as a temporary measure with a hard deadline for patch application per CIS 7.2 (Establish and Maintain a Remediation Process).

Evidence: Before patching, take a full snapshot of `/config/config.xml` and all files in `/config/jdbc/` to preserve credential configuration evidence. Capture the output of `java weblogic.version` to document the pre-patch version string for your incident record. Export WebLogic audit logs covering the exploitation window from `/servers//logs/` — these are needed to establish whether credential harvesting occurred before rotation. If any web shells (.jsp, .jspx) were found in autodeploy or tmp directories, preserve SHA-256 hashes and raw file copies to offline storage before

removal.

Step 4: Recovery — After patching, verify WebLogic server version and patch level through the Oracle inventory tool. Conduct a targeted review of WebLogic deployment directories for unauthorized files or web shells (T1505.003 indicator; D3-SFA). Validate that admin console access requires authentication and is restricted to authorized management networks (NIST AC-3, AC-17). Monitor WebLogic process behavior for 72 hours post-patch using endpoint detection telemetry. Re-enable any isolated services in a controlled, monitored sequence.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST AC-3 (Access Enforcement), NIST AC-17 (Remote Access), NIST SI-2 (Flaw Remediation), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: Run a YARA scan across all WebLogic deployment and temp directories targeting JSP web shell patterns: `yara -r webshell_rules.yar /` using rules from the Neo23x0/signature-base repository (specifically `thor-webshells.yar`). Verify patch level via Oracle OPatch: `/OPatch/opatch lsinventory | grep -i 24839564` (substitute correct CVE patch ID from Oracle CPU). For 72-hour behavioral monitoring without EDR, deploy osquery with a pack querying process ancestry every 60 seconds and pipe to a local log file: `osqueryi --config_path weblogic_monitor.conf`. Validate admin console authentication by attempting an unauthenticated curl request: `curl -v http://:7001/console` — a redirect to login (302) is expected; a 200 response indicates misconfiguration.

Evidence: After patching but before re-enabling network access, capture file system integrity baseline of `` using: `find -type f -exec md5sum {} \; > post_patch_baseline.txt` — diff against a known-good baseline to identify any persistence mechanisms (MITRE ATT&CK T1505.003 — Server Software Component: Web Shell). Collect the Oracle OPatch inventory output as a dated artifact for your change record. Preserve Sysmon or auditd logs covering the 72-hour monitoring window as evidence of clean post-patch behavior — this documentation supports recovery sign-off and insurance/regulatory reporting.

Step 5: Post-Incident — Review your patch management SLA against the two-year gap between CVE assignment (2024) and confirmed exploitation (2026) to determine if deferred patching contributed to exposure (CIS 7.1, CIS 7.2, NIST SI-4). Assess whether WebLogic instances are inventoried and included in your vulnerability scanning scope (CIS 1.1, CIS 7.3, CIS 7.4). Evaluate whether least-privilege network segmentation (NIST AC-6, AC-4) would have limited blast radius had exploitation occurred. Document lessons learned and update WebLogic-specific playbooks.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity

Controls: NIST SI-2 (Flaw Remediation), NIST SI-4 (System Monitoring), NIST AC-4 (Information Flow Enforcement), NIST AC-6 (Least Privilege), 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), CIS 7.3 (Perform Automated Operating System Patch Management), CIS 7.4 (Perform Automated Application Patch Management)

Compensating: For teams without a formal vulnerability management platform, create a WebLogic-specific scan job in OpenVAS or Greenbone Community Edition targeting ports 7001, 7002, and 9002, and schedule it to run weekly. Cross-reference output against a maintained spreadsheet asset inventory (CIS 1.1 minimum viable implementation). To evaluate segmentation gaps, run a traceroute or `nmap --traceroute` from a DMZ or guest network segment toward WebLogic management ports — any successful path that should be blocked indicates a segmentation failure to document in the lessons-learned report. Draft a one-page WebLogic-specific patch SLA addendum that classifies T3/IIOP-exposed instances as Tier 1 assets requiring Critical patch application within 72 hours of Oracle CPU release.

Evidence: Pull vulnerability scan history from your scanner (Nessus, OpenVAS, or equivalent) to document when CVE-2024-21182 was first flagged and whether it appeared in any prior scan reports — this establishes the timeline of awareness versus remediation for the lessons-learned record. Export your CMDB or asset inventory records for all WebLogic instances to verify scan coverage gaps. Retrieve firewall rule history or change logs to assess whether

T3/IIOP (ports 7001, 7002, 9002) were ever explicitly reviewed for internet-facing exposure — absence of a documented review is a finding for the post-incident report.

Detection Guidance

Primary detection signals for CVE-2024-21182 exploitation focus on unauthenticated access patterns and post-exploitation activity. Check WebLogic server logs (server.log, access.log) for requests to T3, T3S, or IIOP listener endpoints from external or unexpected source IPs, particularly without prior authentication events. Look for WebLogic JVM spawning unexpected child processes (cmd.exe, powershell.exe, /bin/bash, curl, wget), this is a strong indicator of remote code execution (T1059, T1190). Search EDR/endpoint telemetry for new .jsp, .war, or .ear files written to WebLogic autodeploy or tmp directories, consistent with web shell staging (T1505.003; system file analysis and file integrity monitoring). Monitor for outbound connections from the WebLogic server process to external IPs on non-standard ports, which may indicate C2 establishment or data staging (T1210). Apply local account monitoring to detect new local accounts or privilege escalation events on WebLogic host systems post-exploitation. If a SIEM is in use, correlate: authentication failures followed immediately by successful privileged actions (post-compromise lateral movement), and unusual use of scripting interpreters on server hosts. Note: no confirmed public IOC hashes, IPs, or domains are available from authoritative sources at this time; behavioral detection and network access pattern monitoring are the primary available methods, with highest confidence signals on: unexpected child process spawning from WebLogic JVM and unauthorized file writes to deployment directories.

Indicators of Compromise

Type	Value	Context	Confidence
URL	`No confirmed IOCs available from authoritative sources at time of writing`	No specific IPs, domains, hashes, or URLs attributed to CVE-2024-21182 exploitation have been published by CISA or NVD as of available source material. Monitor CISA KEV updates and threat intelligence feeds for emerging indicators.	LOW

Framework Mappings

MITRE-ATTACK

- **T1505.003** — Web Shell
- **T1210** — Exploitation of Remote Services
- **T1078** — Valid Accounts
- **T1059** — Command and Scripting Interpreter
- **T1190** — Exploit Public-Facing Application
- **T1133** — External Remote Services

NIST-800-53R5

- **CM-2** — Baseline Configuration
- **CM-7** — Least Functionality
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **SI-7** — Software, Firmware, and Information Integrity
- **AC-6** — Least Privilege
- **SC-7** — Boundary Protection
- **SI-2** — Flaw Remediation
- **AC-2** — Account Management
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **CA-8** — Penetration Testing
- **RA-5** — Vulnerability Monitoring and Scanning
- **AC-17** — Remote Access
- **AC-20** — Use of External Systems
- **AC-3** — Access Enforcement
- **IR-5** — Incident Monitoring

OWASP-TOP10-2021

- **A07:2021** — Identification and Authentication Failures
- **A01:2021** — Broken Access Control

CIS-V8

- **6.3** — Require MFA for Externally-Exposed Applications
- **6.1** — Establish an Access Granting Process
- **6.2** — Establish an Access Revoking Process
- **7.3** — Perform Automated Operating System Patch Management
- **7.4** — Perform Automated Application Patch Management

SOC2-TSC

- **CC6.1** — The entity implements logical access security software, infrastructure, and architectures over protected information assets

HIPAA-SECURITY

- **164.312(a)(1)** — Access Control

ISO-27001-2022

- **A.8.8** — Management of technical vulnerabilities

NIST-CSF-2

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

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1505.003	Web Shell	Persistence
T1210	Exploitation of Remote Services	Lateral-Movement
T1078	Valid Accounts	Defense-Evasion
T1059	Command and Scripting Interpreter	Execution
T1190	Exploit Public-Facing Application	Initial-Access
T1133	External Remote Services	Persistence

Sources

Source	URL	Tier
Security News	https://thehackernews.com/2026/06/oracle-weblogic-cve-2024-21182-ad...	T3
CISA Adds One Known Exploited Vulnerability to Catalog | CISA	https://www.cisa.gov/news-events/alerts/2026/06/01/cisa-adds-one-kn...	T1
CVE-2024-21182: Oracle WebLogic Server Auth Bypass Issue	https://www.sentinelone.com/vulnerability-database/cve-2024-21182/	T3
CISA KEV: Oracle WebLogic CVE-2024-21182 Becomes 2026 ...	https://windowsforum.com/threads/cisa-kev-oracle-weblogic-cve-2024-...	T3
We added Oracle WebLogic Server unspecified vulnerability CVE ...	https://x.com/CISACyber/status/2061512748299665530	T3
NVD	https://nvd.nist.gov/vuln/detail/CVE-2024-21182	T1

Generated 2026-06-03 06:53 UTC by TJS Security Command Center