Oracle Identity Manager: Unauthenticated RCE in IAM Infrastructure

Unofficial AI-assisted Research

Cloud Security Alliance AI Safety Initiative

2026-03-22

This document was generated with AI assistance and has not undergone official CSA review and approval processes.

Key Takeaways

- CVE-2026-21992 is a CVSS 9.8 (Critical) unauthenticated remote code execution vulnerability in Oracle Identity Manager and Oracle Web Services Manager, both components of Oracle Fusion Middleware [1][2].
- The vulnerability is rooted in CWE-306 (Missing Authentication for Critical Function): a REST WebServices endpoint fails to enforce authentication, allowing any network-accessible attacker to execute arbitrary code via HTTP with no credentials required [1][3].
- Oracle issued an out-of-band Security Alert on March 20, 2026 — reportedly only the second such emergency advisory ever issued for Oracle Identity Manager [1][2][8] — suggesting Oracle assessed the exploitation risk as too urgent to defer to the April 2026 CPU cycle.
- This flaw follows CVE-2025-61757, a nearly identical pre-authentication RCE in the same component class that reached CISA's Known Exploited Vulnerabilities catalog in November 2025, establishing a pattern of persistent vulnerability in Oracle's identity platform REST layer [4][5].
- Organizations running Oracle Identity Manager versions 12.2.1.4.0 or 14.1.2.1.0 should treat patch application as an emergency priority, as identity management infrastructure is a high-value target whose compromise grants attackers privileged access to connected enterprise systems and credential stores [1][2].

Background

Oracle Identity Manager — marketed in recent product generations as Oracle Identity Governance (OIG) — is Oracle's enterprise identity provisioning and governance platform within the Fusion Middleware stack. Large enterprises and government agencies deploy it to manage user lifecycle events, enforce role-based access control, conduct access certification campaigns, and govern policy-driven provisioning and de-provisioning across enterprise IT environments. Because Oracle Identity Manager serves as the authoritative source of truth for who holds access to what, a compromise of the platform has consequences that extend far beyond the server itself: an attacker with remote code execution capability on OIM gains potential access to the credential vaults, provisioning workflows, and connected application integrations that govern access across systems managed through Oracle Identity Manager.

Oracle Identity Manager runs on Oracle WebLogic Server, a broadly deployed Java EE application server. The REST WebServices component, which exposes Identity Manager's programmatic management capabilities, is the attack surface implicated in CVE-2026-21992. REST-based management interfaces are commonly exposed to internal network segments and, in some deployment architectures, to internet-facing DMZ environments, making the unauthenticated nature of this vulnerability particularly consequential. Tenable guidance noted that organizations can identify potentially exposed assets by searching for WebLogic Server instances in their external attack surface inventory [5].

The January 2026 Oracle Critical Patch Update addressed several lower-severity flaws in Oracle Identity Manager, including CVE-2025-41249 (CVSS 7.5, via Spring Framework) and CVE-2025-48924 (CVSS 5.3, via Apache Commons Lang), but CVE-2026-21992 was not included in that quarterly cycle [6]. Oracle's decision to issue a standalone Security Alert on March 20, 2026 suggests the company assessed the severity and exploitation risk of this specific flaw as warranting immediate out-of-cycle disclosure rather than deferral to the April 2026 CPU.

Security Analysis

Vulnerability Mechanics

CVE-2026-21992 is classified under CWE-306 (Missing Authentication for Critical Function), indicating that a critical operational function exposed by Oracle Identity Manager's REST WebServices component does not require the caller to authenticate before processing the request [1][3]. The CVSS 3.1 vector string — `CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H` — reflects maximally adverse network reachability factors: network-originated, low complexity, no required privileges, no user interaction, and full high-impact compromise across confidentiality, integrity, and availability dimensions [1]. The resulting base score of 9.8 places CVE-2026-21992 at the top of the critical severity band.

Standard application-level compensating controls — such as service account restrictions or MFA requirements configured within Oracle Identity Manager — do not protect the vulnerable endpoint, as the authentication check itself is absent at the application layer. The NIST NVD description characterizes the vulnerability as "easily exploitable" and capable of enabling "complete takeover" of susceptible instances [3]. However, network-layer controls implemented upstream — such as mTLS termination at an API gateway or WAF-enforced session requirements — can serve as a meaningful compensating control by preventing unauthenticated requests from reaching the vulnerable application layer. Conflicting public reports exist regarding proof-of-concept availability — some sources indicated no public exploit code was available at advisory publication, while others noted the presence of multiple PoC repositories on

GitHub [2][5]. Oracle has declined to confirm in-the-wild exploitation as of the March 20 advisory date, though the out-of-band disclosure timing suggests Oracle's internal threat intelligence assessed a meaningful probability of active or imminent exploitation.

Pattern of Vulnerability in Oracle IAM's REST Layer

CVE-2026-21992 does not exist in isolation. Its immediate predecessor, CVE-2025-61757, carried an identical CVSS score of 9.8 and affected the same REST WebServices component of Oracle Identity Manager across the same two versions (12.2.1.4.0 and 14.1.2.1.0) [4][5]. CVE-2025-61757 was actively exploited in the wild and added to CISA's Known Exploited Vulnerabilities catalog in November 2025, meaning federal agencies were under binding remediation obligations for that prior flaw [4]. Searchlight Cyber researchers, quoted in a Tenable security advisory [5], characterized CVE-2025-61757 as "somewhat trivial and easily exploitable."

The recurrence of a critical unauthenticated RCE in the same component, at the same severity, within months of the previous flaw's active exploitation indicates a structural concern rather than an isolated defect. Whether CVE-2026-21992 represents a bypass of the CVE-2025-61757 patch, a parallel vulnerability in adjacent code paths within the REST layer, or a regression introduced during remediation efforts is not currently confirmed by Oracle. However, the pattern suggests that the underlying authentication enforcement architecture of Oracle Identity Manager's REST WebServices component warrants systematic security review, not only targeted patching of individual CVEs as they surface.

Systemic Risk Context

Identity infrastructure occupies a uniquely privileged position in enterprise security architecture. Attackers who achieve remote code execution on Oracle Identity Manager gain access to a system that, by design, holds provisioning authority over user accounts, group memberships, and entitlements across connected enterprise applications. Depending on organizational deployment, this may include integrations with Active Directory, LDAP directories, cloud service provider identity providers, privileged access management platforms, and line-of-business applications. The blast radius of a successful exploit therefore extends well beyond the compromised server to any system whose access control is managed through Oracle Identity Manager.

This risk profile places CVE-2026-21992 within a broader pattern of identity infrastructure targeting observed throughout early 2026. CSA's concurrent threat intelligence analysis indicates that identity infrastructure has been a recurring, high-priority target in observed exploitation activity during this period; organizations should consider CVE-2026-21992 within that wider context [7]. Organizations that have not yet fully remediated CVE-2025-61757, or that did not verify their Oracle Identity Manager deployments were included in January 2026 CPU patching, should treat the March 20 advisory as an opportunity to audit the completeness of their historical remediation posture alongside applying the current emergency patch.

Recommendations

Immediate Actions

The highest priority action for any organization operating Oracle Identity Manager 12.2.1.4.0 or 14.1.2.1.0 is to apply the out-of-band Oracle Security Alert patch issued March 20, 2026 as rapidly as possible [2]. Patches are available through Oracle's Fusion Middleware Patch Availability Document (KB878741). Given that the predecessor CVE (CVE-2025-61757) was actively exploited and technically trivial to leverage, organizations should not wait for a scheduled maintenance window if the affected system is network-accessible from any untrusted segment.

Before patching or as a concurrent measure, organizations should enumerate all Oracle Identity Manager deployments to verify which versions are running and whether the REST WebServices component is reachable from internal networks, DMZ segments, or the internet. Tenable's guidance suggests using attack surface management tooling to identify internet-facing WebLogic Server instances as a proxy for potentially exposed Oracle Identity Manager deployments [5]. Any instances found to be externally reachable should be isolated at the network perimeter immediately, with REST endpoint access restricted to explicitly authorized management networks pending patch application.

Organizations should also review server logs on affected Identity Manager instances for evidence of anomalous unauthenticated requests to REST endpoints, unusual provisioning activity, new account creation events, or privilege escalation chains that may indicate exploitation prior to discovery of this advisory. Given the precedent of active exploitation of the prior related CVE, a presumption of potential prior compromise is appropriate for organizations that have had internet-accessible Oracle Identity Manager instances running unpatched versions.

Short-Term Mitigations

Beyond emergency patching, organizations should implement layered network controls to restrict access to Oracle Identity Manager's administrative and REST interfaces. Specifically, web application firewall rules or API gateway policies should enforce authenticated sessions at the perimeter before requests reach the REST WebServices component, providing a defense-in-depth layer that compensates for application-level authentication failures. Internal network segmentation should ensure that Oracle Identity Manager is accessible only from explicitly defined management networks and application integration endpoints, not from general user network segments.

Security operations teams should deploy or update detection coverage for anomalous activity originating from Oracle Identity Manager hosts, including unexpected outbound network connections, process execution patterns inconsistent with normal WebLogic operation, and unusual provisioning API calls that lack associated authenticated user sessions. Detection logic should specifically address cases where the REST API is invoked from unexpected source addresses or without standard session authentication headers, consistent with the attack patterns associated with unauthenticated interface exploitation and administrative channel manipulation.

For organizations using Tenable, plugin updates covering active scanning for CVE-2026-21992 were being released as of the March 20 advisory date and should be incorporated into scheduled vulnerability scan configurations [5].

Strategic Considerations

The recurrence of critical pre-authentication RCE in Oracle Identity Manager's REST layer invites a broader strategic question about the risk posture associated with large, monolithic on-premises identity management platforms. Organizations should evaluate whether their Oracle Identity Manager deployment architectures adequately restrict the attack surface of the REST interface, and consider whether the administrative management surface of identity infrastructure should be subject to the same zero-trust access principles applied to other critical administrative interfaces — specifically, requiring strong authentication, just-in-time access, and full session logging for any API-level access to the identity management platform.

Organizations should also assess their vendor notification and emergency patch response processes. Oracle's out-of-band advisory represents an unusual step that signals elevated urgency, and organizations whose patching workflows default to quarterly patch cycles may have structural gaps in their capacity to respond to out-of-band advisories within a timeframe commensurate with the risk. Formalizing an emergency patch tier — with defined escalation, approval, and deployment timelines for CVSS 9.0+ out-of-band advisories from critical vendors — is a governance improvement worth prioritizing in light of this incident.

Looking further ahead, organizations that rely on Oracle Identity Manager as a primary provisioning and governance platform should include it in their enterprise security architecture review cadence, with specific attention to the REST API threat model, authentication boundary integrity, and the completeness of logging and behavioral detection for unusual provisioning activity. The persistence of critical vulnerabilities in this component suggests that passive patching alone is insufficient; active security architecture validation of the identity platform's network exposure and access control boundaries is warranted.

CSA Resource Alignment

CVE-2026-21992 directly implicates several domains addressed in CSA's published guidance frameworks. The Cloud Controls Matrix (CCM) addresses identity and access management governance under the IAM control domain, with specific controls covering privileged access management, authentication enforcement, and session management — all of which are relevant to hardening Oracle Identity Manager's administrative interfaces and REST endpoint security posture [11]. Organizations using the CCM as a compliance reference should map their Oracle Identity Manager deployment controls against the IAM domain controls as part of their post-patch posture review.

The AI Identity and Credential Management (AICM) framework, which extends CCM in the context of AI-integrated enterprise environments and serves as the authoritative reference for AI-specific identity and credential controls [10], provides guidance on securing identity management infrastructure that may be leveraged by or integrated with AI systems. In organizations where Oracle Identity Manager governs service account provisioning for AI agents or AI platform integrations, an unauthenticated RCE in identity infrastructure threatens the credential and access boundaries that constrain AI agent behavior in enterprise environments. Such organizations should treat patching Oracle Identity Manager as directly relevant to their AI security posture, not solely as a traditional IT remediation action.

The MAESTRO framework for agentic AI threat modeling identifies identity infrastructure compromise as a high-severity threat vector against AI agent deployments, particularly in scenarios where AI agents rely on enterprise identity services for authentication, authorization, and service-to-service credential management [9]. A compromised Oracle Identity Manager instance can be used to provision unauthorized service accounts, modify role assignments for existing AI agent identities, or tamper with provisioning policies in ways that silently expand AI agent privileges in connected systems. Security teams conducting MAESTRO-aligned threat modeling of their AI agent deployments should explicitly include the identity management platform in their threat surface analysis.

CSA's Zero Trust guidance is directly applicable to the network access controls recommended in this note. The principle of never-trust-always-verify applied to Oracle Identity Manager's REST interface means requiring explicit authentication at every access boundary rather than relying on network perimeter trust to protect an administrative API. Implementing zero-trust network segmentation around Oracle Identity Manager — restricting REST API access to verified management hosts over authenticated, encrypted channels — substantially reduces the exploitability of unauthenticated vulnerabilities at the application layer, because the attacker's ability to reach the vulnerable endpoint is constrained regardless of whether application-layer authentication is enforced.

Organizations should also consult CSA's STAR (Security Trust Assurance and Risk) registry [12] when evaluating the security posture of any cloud-delivered identity management components that complement or integrate with their Oracle Identity Manager deployments, as third-party identity platform security postures directly affect the overall enterprise IAM risk profile.

References

[1] Oracle Corporation, "Oracle Security Alert Advisory – CVE-2026-21992," Oracle Security Alerts, March 20, 2026. https://www.oracle.com/security-alerts/alert-cve-2026-21992.html

[2] S. Gatlan, "Oracle pushes emergency fix for critical Identity Manager RCE flaw," BleepingComputer, March 20, 2026. https://www.bleepingcomputer.com/news/security/oracle-pushes-emergency-fix-for-critical-identity-manager-rce-flaw/

[3] National Institute of Standards and Technology, "CVE-2026-21992 Detail," National Vulnerability Database, March 20, 2026. https://nvd.nist.gov/vuln/detail/CVE-2026-21992

[4] Cybersecurity and Infrastructure Security Agency, "Known Exploited Vulnerabilities Catalog – CVE-2025-61757," CISA KEV, November 2025. https://www.cisa.gov/known-exploited-vulnerabilities-catalog

[5] Tenable, "CVE-2026-21992: Critical Out-of-Band Oracle Identity Manager and Oracle Web Services Manager Remote Code Execution Vulnerability," Tenable Blog, March 2026. https://www.tenable.com/blog/cve-2026-21992-critical-out-of-band-oracle-identity-manager-and-oracle-web-services-manager

[6] Oracle Corporation, "Oracle Critical Patch Update Advisory – January 2026," Oracle Security Alerts, January 2026. https://www.oracle.com/security-alerts/cpujan2026.html

[7] Cloud Security Alliance AI Safety Initiative, "Daily Intelligence Report – March 22, 2026," CSA Internal Analysis, 2026.

[8] Security Boulevard, "CVE-2026-21992: Critical Out-of-Band RCE," Security Boulevard, March 2026. https://securityboulevard.com/2026/03/cve-2026-21992-critical-out-of-band-oracle-identity-manager-and-oracle-web-services-manager-remote-code-execution-vulnerability/

[9] Cloud Security Alliance, "MAESTRO: AI Agentic Security Threat Modeling Framework," Cloud Security Alliance AI Safety Initiative, 2025.

[10] Cloud Security Alliance, "AI Identity and Credential Management (AICM) Framework," Cloud Security Alliance, 2025.

[11] Cloud Security Alliance, "Cloud Controls Matrix (CCM) v4.0," Cloud Security Alliance, 2021. https://cloudsecurityalliance.org/research/cloud-controls-matrix/

[12] Cloud Security Alliance, "Security Trust Assurance and Risk (STAR) Program," Cloud Security Alliance. https://cloudsecurityalliance.org/star/