Oracle Identity Manager & Web Services Manager RCE Vulnerability

TL;DR

Oracle Identity Manager and Oracle Web Services Manager contain a remote code execution vulnerability (CVE-2026-21992) that can be exploited without authentication.

An attacker could gain full control of affected systems depending on user privileges. There are no reports of active exploitation yet.

Overview

There is a vulnerability in Oracle Identity Manager and Oracle Web Services Manager that allows remote code execution (CVE-2026-21992, CVSS: TBD). The flaw can be exploited without authentication, which means an attacker does not need valid credentials to trigger it.

Affected Products

- Oracle Identity Manager – versions 12.2.1.4.0, 14.1.2.1.0
- Oracle Web Services Manager – versions 12.2.1.4.0, 14.1.2.1.0

If exploited, a threat actor could run code on the affected system. That access could be used to install malware, change or delete data, or create new accounts. The level of control depends on the privileges tied to the application, but in many environments this could lead to full system compromise.

If CVE-2026-21992 is exploited, a threat actor could take control of the system, access or change sensitive data, and create new accounts to stay in the environment. If these systems are exposed, this gives them a clear way in. Aspire recommends patching immediately.

Aspire Protects

- **Patch** - Apply Oracle patches immediately after testing. See Oracle's security advisory for more information.
- Limit privileges on service accounts and applications.
- Monitor internet-facing Oracle services for unusual activity.
- Run regular vulnerability scans against Oracle systems.
- Segment critical systems from public-facing applications.

TTPs to Watch

Initial Access

- Exploit Public-Facing Application [T1190] – The attacker may exploit an exposed Oracle application to gain unauthorized access without needing credentials.

IoCs

There are no known IoCs at this time. Aspire is actively monitoring and will notify customers if any are found. For more details on how we can help protect your organization, contact Aspire's Customer Success Management team.

Targeted Industries

Organizations that rely on Oracle identity and middleware platforms may be impacted, including:

- Education
- Energy
- Finance
- Healthcare
- Legal
- Manufacturing
- Public Sector
- Retail

Aspire Service Offerings

- **Aspire Managed XDR (MXDR)**
  - Aspire Managed XDR (MXDR) combines next-generation eXtended Detection and Response (XDR) technology, a 24x7 security operations center (SOC), and the expertise of a US-based team of security professionals to identify and respond to threats across a broader attack surface.
  - Building on the existing capabilities of Managed Detection and Response (MDR), Aspire Managed XDR integrates and correlates telemetry from endpoints, network, cloud, email, identity, and more. This advanced platform creates valuable context enabling end-to-end visibility across all threat vectors.

  - Experienced security analysts and incident responders deliver 24x7 threat detection, analysis, and investigations – with both automated and human-led response actions to quickly mitigate cyber attacks.
- **Aspire Incident Response**
  - The ability to respond effectively to data breaches is critical to every organization. When attacks occur, IT leaders need a process that will ultimately maintain business continuity, protect the company reputation, and avoid fines, legal fees, and remediation costs.
  - Aspire offers incident response services to help you prepare for, manage, and recover from data breaches and network attacks. An experienced team uses industry-leading threat intelligence and the most current security technology to quickly respond to attacks, reduce damage, and minimize exposure.

Supporting Documentation

Oracle Security Alert Advisory - CVE-2026-21992

NVD - CVE-2026-21992

Oracle vulnerability (CVE-2026-21992) impacts core products | SOPHOS