Attackers Target Oracle WebLogic Servers Through Unauthenticated Vulnerability

***Author**: Portia S. Cole – CTI Researcher*

TL;DR

CVE-2024-21182 (CVSS 7.5) is an actively exploited Oracle WebLogic Server vulnerability that allows an unauthenticated attacker to access sensitive data through exposed T3 or IIOP services.

The vulnerability has been added to CISA's Known Exploited Vulnerabilities (KEV) Catalog, and organizations should patch affected systems immediately.

Overview

The Cybersecurity and Infrastructure Security Agency (CISA) added CVE-2024-21182 (CVSS 7.5) to its Known Exploited Vulnerabilities (KEV) Catalog after confirming active exploitation in the wild. The vulnerability affects Oracle WebLogic Server and allows an unauthenticated attacker with network access through T3 or IIOP protocols to access sensitive information stored within affected environments.

Affected Products

- Oracle WebLogic Server 12.2.1.4.0
- Oracle WebLogic Server 14.1.1.0.0

According to Oracle, successful exploitation may result in unauthorized access to critical data or all information accessible through the affected WebLogic Server instance. While public reporting has not disclosed specific exploitation details, Oracle WebLogic vulnerabilities are often targeted by threat actors for initial access, data theft, crypto mining operations, and ransomware deployment. Aspire recommends that organizations with internet-facing WebLogic services should prioritize patching and review systems for signs of suspicious activity.

Aspire Protects

- **Patch** - Apply Oracle's July 2024 security updates immediately.
- Identify and inventory all Oracle WebLogic Server instances within the environment.
- Restrict access to T3 and IIOP services where business requirements permit.
- Review firewall rules and limit exposure of WebLogic services to trusted networks.

- Monitor WebLogic logs for unusual connections, authentication activity, or administrative actions.
- Review user accounts and permissions for unauthorized changes.
- Conduct threat hunting activities on exposed WebLogic systems.

TTPs to Watch

Initial Access

- Exploit Public-Facing Application [T1190] – The threat actor may exploit a vulnerable Oracle WebLogic Server instance exposed to the network to gain unauthorized access.

Collection

- Data from Information Repositories [T1213] – The threat actor may access or collect sensitive information stored within the affected WebLogic environment following successful exploitation.

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

Oracle WebLogic Server is commonly used across:

- 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 Critical Patch Update Advisory - July 2024

CVE Record: CVE-2024-21182