Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

CVE-2025-61757: Oracle Identity Manager Pre-Auth RCE Under Active Attack

Date of Publication	Admiralty Code	TA Number
November 28, 2025	A1	TA2025364

Summary

First Seen: August 30, 2025
Affected Product: Oracle Identity Manager (OIM)
Impact: CVE-2025-61757 is a critical authentication-bypass vulnerability in Oracle Identity Manager that allows unauthenticated attackers to access protected REST endpoints and achieve remote code execution. The flaw stems from regex-based allow-listing in the SecurityFilter, enabling simple URI manipulations such as ;.wadl or ?WSDL to bypass authentication. The vulnerability was actively exploited as a zero-day months before Oracle's October 2025 patch. Organizations using affected versions face high risk of full system compromise and must apply patches and restrict exposure immediately.

CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2025-61757	Oracle Fusion Middleware Missing Authentication for Critical Function Vulnerability	Oracle Identity Manager (OIM), part of Oracle Fusion Middleware	✓	✓	✓

Vulnerability Details

#1

CVE-2025-61757 is a critical authentication-bypass vulnerability in Oracle Identity Manager, a core component of Oracle Fusion Middleware used for enterprise identity governance. Assigned a CVSS score of 9.8, the flaw enables unauthenticated remote code execution through improperly protected REST API endpoints. The vulnerability arises from weaknesses in the product's SecurityFilter, which relies on regex-based allow-listing instead of strict per-route access controls. As a result, attackers can append matrix parameters such as ;.wadl or query strings like ?WSDL to request URIs, causing the filter to misclassify protected endpoints as publicly accessible.

#2 Once authentication is bypassed, attackers can invoke internal management APIs, most notably a Groovy script compilation endpoint intended only for syntax checking. Although designed for validation, this endpoint compiles submitted scripts, and Groovy's support for compile-time annotation execution allows malicious behavior to run during compilation itself. This gives adversaries a pathway to remote code execution without requiring the script to execute normally, enabling full system compromise and unauthorized access to identity-governed resources.

#3 Evidence confirms the vulnerability was exploited as a zero-day. SANS Internet Storm Center honeypots recorded active exploitation attempts between August 30 and September 9, 2025, well before Oracle issued a fix in the October 2025 Critical Patch Update. Organizations running affected Oracle Identity Manager versions face significant risk if systems remain unpatched, especially when REST endpoints are internet-exposed.

#4 The pre-authentication nature of the vulnerability over HTTP dramatically increases exposure for perimeter-accessible instances. Its trivial exploitation method, zero-day status, and confirmed active exploitation, collectively elevate this vulnerability to maximum priority for remediation.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2025-61757	Oracle Identity Manager Versions 12.2.1.4.0 and 14.1.2.1.0	cpe:2.3:a:oracle:identity_manager:*:*:*:*:*:*:*:*	CWE-306

Recommendations

Apply Critical Patch Update Immediately: Install Oracle's October 2025 Critical Patch Update on all affected Oracle Identity Manager instances. This is the only definitive fix for the SecurityFilter authentication-bypass flaw. Prioritize systems with internet-facing REST endpoints.

Block Malicious URI Patterns: Configure WAFs, reverse proxies, and load balancers to block or sanitize requests containing ;.wadl, .wadl, or ?WSDL. These patterns directly trigger the SecurityFilter regex bypass that enables unauthenticated access.

Restrict Sensitive REST Endpoints: Limit or disable access to the Groovy script compilation endpoint (/groovyscriptstatus) and related Application Management APIs. These endpoints enable remote code execution once authentication is bypassed.

Review Logs for Exploitation Attempts: Search HTTP access logs for requests ending in ;.wadl or ?WSDL, and especially POST requests of ~556 bytes to the Groovy script–status endpoint. These are strong indicators of active exploitation attempts tied to CVE-2025-61757.

Remove Internet Exposure of OIM: Immediately isolate or firewall Oracle Identity Manager servers exposed to the public internet. Due to the pre-authentication nature of the flaw, any unauthenticated network access presents a severe compromise risk.

Potential MITRE ATT&CK TTPs

TA0043 Reconnaissance	**TA0042** Resource Development	**TA0001** Initial Access	**TA0002** Execution
TA0006 Credential Access	**TA0005** Defense Evasion	**T1588** Obtain Capabilities	**T1595** Active Scanning
T1190 Exploit Public-Facing Application	**T1059** Command and Scripting Interpreter	**T1552** Unsecured Credentials	**T1548** Abuse Elevation Control Mechanism

T1203 Exploitation for Client Execution	T1036 Masquerading	T1548.002 Bypass User Account Control	T1068 Exploitation for Privilege Escalation
T1595.002 Vulnerability Scanning	T1588.006 Vulnerabilities	T1588.005 Exploits	

Indicators of Compromise (IOCs)

TYPE	VALUE
IPv4	89[.]238[.]132[.]76, 185[.]245[.]82[.]81, 138[.]199[.]29[.]153

Patch Link

https://www.oracle.com/security-alerts/cpuoct2025.html

References

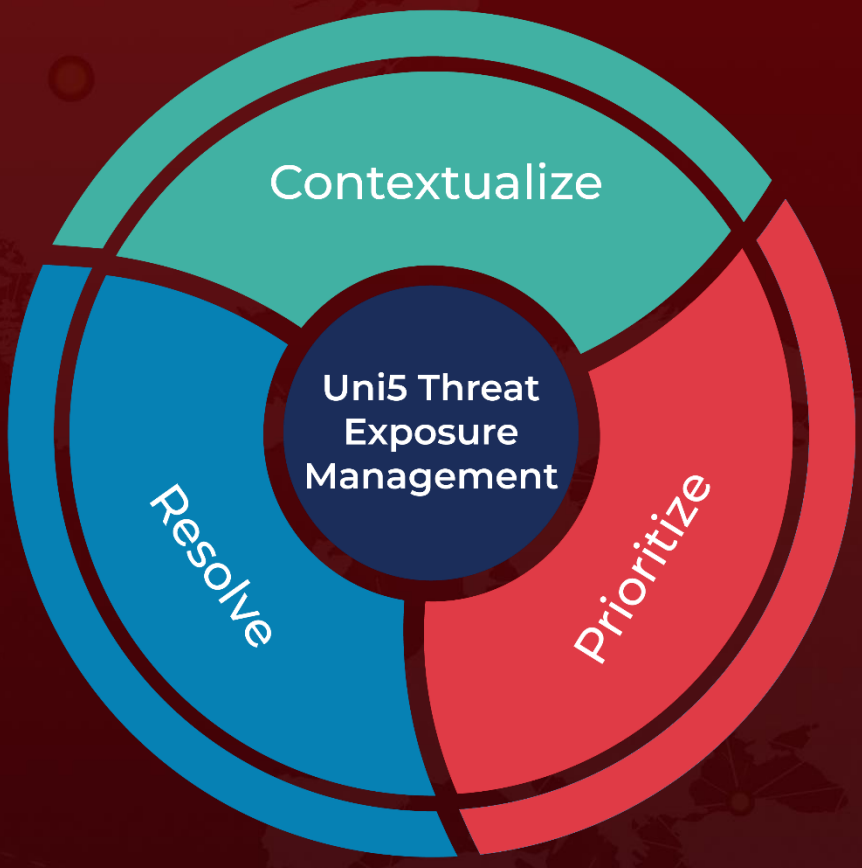
https://isc.sans.edu/diary/rss/32506

https://slcyber.io/research-center/breaking-oracles-identity-manager-pre-auth-rce/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

November 28, 2025 . 8:30 AM

More at www.hivepro.com