CVE-2025-61757

Oracle Identity Manager Pre-Authentication Remote Code Execution

CVSS Score 9.8 (Critical)
Published 2025-12-07
Classification TLP:CLEAR
Exploitation Active Zero-Day (Aug 2025+)

Intruvent Technologies

INT-VA-2025-CVE-2025-61757-v1.0

1 Executive Summary

9.8 Critical Severity
Pre-Authentication RCE · CWE-306
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Active Zero-Day Exploitation
CVE-2025-61757 has been actively exploited since late August 2025, weeks before Oracle released a patch. CISA added this vulnerability to the KEV catalog on November 21, 2025, with a remediation deadline of December 12, 2025. Over 300,000 attack attempts have been recorded globally across 18+ countries.

CVE-2025-61757 is a critical pre-authentication remote code execution vulnerability in Oracle Identity Manager (OIM), part of Oracle Fusion Middleware. The flaw exists in the REST WebServices component, where attackers can bypass authentication filters by appending metadata-style suffixes (`;.wadl` or `;WADL`) to protected API endpoints. Once authentication is bypassed, attackers exploit a Groovy script compilation endpoint to achieve arbitrary code execution through annotation-processing abuse.

Key Facts

CVE ID	CVE-2025-61757
Vendor	Oracle (Fusion Middleware)
CVSS v3.1	9.8 (Critical)
CWE	CWE-306: Missing Authentication for Critical Function
Attack Vector	Network (Remote, No Authentication)
Vulnerable Component	REST WebServices / Groovy Script Endpoint
Exploitation	Active zero-day since August 2025
CISA KEV	Added November 21, 2025 (Due: Dec 12, 2025)
Global Impact	300,000+ attack attempts in 18+ countries

2 Threat Actor Intelligence

No Attributed Threat Actor Exploitation
As of December 7, 2025, no specific threat actor or APT group has been publicly attributed to the exploitation of CVE-2025-61757. However, the scale and sophistication of attacks suggest organized exploitation campaigns. SANS Internet Storm Center observed exploitation attempts in honeypot systems from August 30 to September 8, 2025—occurring before Oracle released its patch—indicating zero-day awareness among threat actors.

300,000+ ATTACK ATTEMPTS
18+ COUNTRIES TARGETED
3 PRIMARY SECTORS

Observed Attack Patterns

According to Imperva threat research, attacks have concentrated on organizations in the **computing**, **healthcare**, and **business services** sectors. The highest attack volumes were observed in the **United States** and **France**.

Attack Infrastructure Observations

Indicator	Type	Context
`89.238.132.76`	IPv4	Observed exploitation attempts
`185.245.82.81`	IPv4	Observed exploitation attempts
`138.199.29.153`	IPv4	Observed exploitation attempts
`Chrome/68.0.3112.113`	User-Agent	Outdated (2017) browser signature – anomalous in 2025
`506 bytes`	Payload Size	Consistent POST body size in exploitation attempts

Assessment: The consistent use of an outdated Chrome user-agent string (from 2017) across multiple source IPs suggests automated tooling or a shared exploitation framework among attackers. The uniform 506-byte payload size indicates standardized exploit code.

3 Affected Products

Vulnerable Versions

Product	Vulnerable Versions	Fixed Version
Oracle Identity Manager	12.2.1.4.0	**October 2025 CPU**
Oracle Identity Manager	14.1.2.1.0	**October 2025 CPU**

Enterprise Impact
Oracle Identity Manager is a core enterprise identity governance solution deployed widely across Fortune 500 companies, government agencies, and healthcare organizations. Compromise of OIM can lead to:

- Mass creation of privileged accounts
- Tampering with identity provisioning workflows
- Bypass of MFA and SSO authentication mechanisms
- Lateral movement to connected directory services (AD, LDAP)
- Compromise of integrated SaaS platforms

4 Technical Analysis

Vulnerability Mechanism

The vulnerability exploits two weaknesses in Oracle Identity Manager's REST API implementation:

1. Authentication Bypass
OIM's REST security filters incorrectly handle URL paths containing metadata-style suffixes. By appending `;.wadl` or `;WSDL` to protected endpoints, attackers trick the filter into treating them as publicly accessible WADL/WSDL descriptor requests, bypassing authentication entirely.

2. Groovy Compile-Time Code Execution
Once authenticated access is bypassed, attackers target the Groovy script validation endpoint. While this endpoint only compiles scripts (without executing them), Groovy's annotation-processing and AST (Abstract Syntax Tree) transform features allow code execution during compilation. Malicious annotations trigger execution before the "no-runtime-execution" restriction applies.

CVE-2025-61757 Exploitation Chain

STEP 1: AUTHENTICATION BYPASS
- Append `;.wadl` or `;WSDL` to protected REST endpoint
- Security filter misclassifies request as metadata descriptor
- Unauthenticated access granted to protected API

↓

STEP 2: TARGET GROOVY ENDPOINT
- POST to `/oak/governance/.../groovyscriptstatus;.wadl`
- Endpoint accepts Groovy script for "validation"
- Script is compiled server-side (not executed at runtime)

↓

STEP 3: ANNOTATION ABUSE
- Craft Groovy script with malicious annotation processors
- AST transforms execute during compilation phase
- Bypass runtime execution restrictions

↓

STEP 4: RCE ACHIEVED
- Arbitrary code execution on WebLogic/JVM server
- Create privileged accounts, install backdoors
- Pivot to connected identity infrastructure

Vulnerable Endpoints

Endpoint	Method	Purpose
`/oak/governance/api/internalmgmt/api/v1/application/groovyscriptstatus`	POST	Groovy script validation – Primary RCE vector
`/oak/governance/api/internalmgmt/templates`	GET/POST	Application management templates

5 Exploitation Timeline

SANS Internet Storm Center documented zero-day exploitation well before Oracle's patch release.

Date	Event	Details
Aug 30 – Sep 8, 2025	Zero-Day Exploitation	SANS honeypots record multiple exploitation attempts from various IPs using same user-agent and 506-byte payloads
Oct 21, 2025	Patch Released	Oracle addresses vulnerability in October 2025 Critical Patch Update
Nov 21, 2025	CISA KEV Added	Added to Known Exploited Vulnerabilities catalog after exploitation validation
Dec 12, 2025	CISA Deadline	Federal agencies required to complete remediation

Global Attack Statistics
According to Imperva Threat Research, over **300,000 attack attempts** have been recorded globally, targeting organizations in **18+ countries**. The highest concentration of attacks targeted the United States and France, with primary focus on computing, healthcare, and business sectors.

6 Detection

Indicators of Compromise

Malicious IP Addresses
The following IPs were observed in exploitation attempts (SANS ISC):

IP Address	Context
`89.238.132.76`	Observed exploitation attempts (Aug-Sep 2025)
`185.245.82.81`	Observed exploitation attempts (Aug-Sep 2025)
`138.199.29.153`	Observed exploitation attempts (Aug-Sep 2025)

User-Agent Fingerprint

```
Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/68.0.3112.113 Safari/537.36
```

Note: Chrome 68.x was released in 2017. This severely outdated browser version is anomalous in 2025 traffic and serves as a detection indicator.

Request Characteristics

Indicator	Value	Detection Method
URL Suffix	`;.wadl` or `;WSDL`	Wildfire/URL pattern matching
HTTP Method	POST	Filter POST requests to groovyscriptstatus
Content-Length	~506 bytes	Flag POST requests with this payload size

Detection Queries
SPLUNK: REPEAT AUTHENTICATION BYPASS ATTEMPTS

```
index=web_logs sourcetype=access_combined | where match(uri_path, "(?i)/oak/governance/.*groovyscriptstatus") | where
match(uri_path, "(?i);.wadl|;WSDL") | where http_method="POST" | stats count by src_ip, uri_path, http_user_agent, bytes_in |
where bytes_in >= 500 AND bytes_in <= 600
```

KQL: MICROSOFT SENTINEL / DNS EXFILTRATION DETECTION

```
CommonSecurityLog | where RequestURL contains "groovyscriptstatus" | where RequestURL matches regex @"(?i);.wadl|;WSDL" |
where RequestMethod == "POST" | project TimeGenerated, SourceIP, RequestURL, RequestClientApplication, SentBytes | where SentBytes
between (500 .. 600)
```

7 Remediation

PATCH IMMEDIATELY Active zero-day · CISA KEV deadline Dec 12, 2025

Patching Guidance

Product	Current Version	Action Required
Oracle Identity Manager	12.2.1.4.0	**Apply October 2025 CPU**
Oracle Identity Manager	14.1.2.1.0	**Apply October 2025 CPU**

Immediate Mitigations

If patching cannot be completed immediately, implement these compensating controls:

WAF RULE: BLOCK AUTHENTICATION BYPASS SUFFIXES

```
# Block requests containing bypass suffixes to OIM endpoints SecRule REQUEST_URI "@rx /oam/governance/.*(;|%3[Bb]).*(.wadl|WSDL)" \
"id:1001,phase:1,deny,status:403,log,msg:'CVE-2025-61757 - OIM Auth Bypass Attempt'"
```

NETWORK ACL: BLOCK KNOWN MALICIOUS IPS

```
# Block IPs associated with exploitation attempts iptables -A INPUT -s 89.238.132.76 -j DROP iptables -A INPUT -s 185.245.82.81 -j
DROP iptables -A INPUT -s 138.199.29.153 -j DROP
```

Additional Hardening

- **Restrict OIM Management Access:** Limit access to OIM administrative interfaces to trusted networks only
- **Enable Enhanced Logging:** Configure verbose logging for REST API access attempts
- **Monitor Groovy Endpoint:** Alert on any POST requests to groovyscriptstatus endpoint
- **User-Agent Filtering:** Block requests with Chrome 68.x user-agent at edge
- **Constrain POST Size:** Limit POST request body size to OIM endpoints where practical

Critical Warning
This vulnerability is particularly dangerous due to its simplicity compared to typical Oracle CVEs. The straightforward exploitation chain makes it highly susceptible to widespread abuse. Organizations running unpatched Oracle Identity Manager should assume they may already be compromised and conduct thorough forensic investigation.

Post-Compromise Actions

If exploitation is suspected or confirmed:

1. **Audit all OIM accounts** – Check for unauthorized privileged account creation
2. **Review provisioning workflows** – Identify any tampered identity workflows
3. **Check connected systems** – Audit AD, LDAP, and integrated SaaS platforms for unauthorized changes
4. **Review WebLogic logs** – Search for evidence of backdoor installation
5. **Reset credentials** – Change passwords for all OIM administrative accounts
6. **Forensic investigation** – Assess lateral movement and data exfiltration

8 References

Oracle Critical Patch Update – October 2025

Horizon3.ai – CVE-2025-61757 Technical Analysis

CISA Known Exploited Vulnerabilities Catalog

BleepingComputer – CISA Warns of OIM Exploitation

The Hacker News – Oracle Identity Manager Zero-Day

Imperva – CVE-2025-61757 Attack Statistics

SecurityWeek – CISA Confirms OIM Exploitation