Hive Pro

Threat Level

Red

Hiveforce Labs

# THREAT ADVISORY

## VULNERABILITY REPORT

# CVE-2026-21962: Critical Oracle WebLogic Proxy Plug-in Flaw Exploited in the Wild


| Date of Publication | Admiralty Code | TA Number |
| --- | --- | --- |
| August 26, 2026 | A1 | TA2026246 |

# Summary

**First Seen:** January 20, 2026
**Affected Products:** Oracle HTTP Server, Oracle Weblogic Server Proxy Plug-in product of Oracle Fusion Middleware
**Impact:** CVE-2026-21962 is a maximum-severity (CVSS 10.0) improper access-control flaw in Oracle HTTP Server and the WebLogic Server Proxy Plug-in for Apache and IIS, letting an unauthenticated attacker send crafted HTTP requests to read, create, modify, or delete data through the edge proxy, with a scope change that reaches backend applications. It affects only the proxy plug-in layer (versions 12.2.1.4.0, 14.1.1.0.0, 14.1.2.0.0 for Apache/OHS; 12.2.1.4.0 for IIS), making it primarily an internet-facing edge risk. Oracle fixed it in the January 2026 Critical Patch Update, so it is not a zero-day, but a public PoC drove exploitation from late January onward, prioritize patching of internet-facing instances.

## CVE

| CVE | NAME | AFFECTED PRODUCT | ZERO-DAY | CISA KEV | PATCH |
|---|---|---|---|---|---|
| CVE-2026-21962 | Oracle HTTP Server and Oracle Weblogic Server Proxy Plug-in Improper Access Control Vulnerability | Oracle HTTP Server, Oracle WebLogic Server Proxy Plug-in (Oracle Fusion Middleware) | ✗ | ✓ | ✓ |

# Vulnerability Details

**#1**

CVE-2026-21962 is a maximum-severity access control vulnerability (CVSS 10.0, CWE-284) in Oracle's web proxy software, specifically the Oracle HTTP Server and the WebLogic Server Proxy Plug-in that sits at the network edge and forwards incoming web traffic to backend WebLogic application servers. An attacker on the internet can reach the proxy without any credentials and send specially crafted HTTP requests, and from there read, create, modify, or delete data passing through it. Because the flaw carries a scope change, the impact can extend beyond the proxy to the applications and services behind it.

**#2**

A key scoping point is that this does not affect every WebLogic deployment, only the proxy plug-in layer used with Apache HTTP Server or Microsoft IIS. The affected versions are 12.2.1.4.0, 14.1.1.0.0, and 14.1.2.0.0 for the Apache HTTP Server plug-in variant, and 12.2.1.4.0 only for the IIS variant. This makes it primarily an edge-exposure risk, so checks should focus on internet-facing and DMZ systems running the proxy rather than internal application servers.

**#3**

The patch preceded any observed exploitation, so this was not a zero-day; however, a public proof-of-concept appeared around January 22, 2026, and honeypot telemetry recorded exploitation attempts almost immediately, with further exploitation reporting through mid-2026. CISA added the vulnerability to its Known Exploited Vulnerabilities catalog only on August 24, 2026, roughly seven months later, with a remediation due date of August 27, 2026, a notable lag that confirms active exploitation while illustrating that KEV listing trailed the real-world evidence.

**#4**

Remediation is straightforward but should be treated as a priority. Applying Oracle's January 2026 Critical Patch Update is the only complete fix, and it needs to reach all affected nodes, including failover and non-production systems. Until patching is complete, restrict network access to the affected proxy ports so they are reachable only from trusted sources, and isolate edge proxy hosts from the backend WebLogic clusters they serve.

# Vulnerability

| CVE ID | AFFECTED PRODUCTS | AFFECTED CPE | CWE ID |
|---|---|---|---|
| CVE-2026-21962 | Oracle HTTP Server, Oracle WebLogic Server Proxy Plug-in for Apache HTTP Server (12.2.1.4.0, 14.1.1.0.0, 14.1.2.0.0); WebLogic Server Proxy Plug-in for Microsoft IIS (12.2.1.4.0) | cpe:2.3:a:oracle:http_server:*:*:*:*:*:*:*:*; cpe:2.3:a:oracle:weblogic_server_proxy_plug-in:*:*:*:*:*:*:*:* | CWE-284 |

# Recommendations

**Apply the Oracle January 2026 Critical Patch Update Immediately:** Install the security patches delivered in the Oracle Critical Patch Update of January 2026 for all affected WebLogic Server Proxy Plug-in and Oracle HTTP Server instances without delay. Patching is the definitive remediation for this vulnerability, and it should be applied to versions 12.2.1.4.0, 14.1.1.0.0, and 14.1.2.0.0 of the Apache HTTP Server plug-in and to version 12.2.1.4.0 of the Microsoft IIS plug-in. Follow the organization's patch testing and change-management procedures to minimize operational disruption while treating this deployment as high priority.

**Prioritize Internet-Facing Instances:** Identify every affected instance that is reachable from untrusted networks and remediate those first, since the vulnerability is exploitable by an unauthenticated remote attacker and is confirmed under active exploitation.

**Apply Vendor Workarounds Where Patching Must Be Delayed:** If immediate patching is not feasible, follow the vendor's published workaround guidance in the Critical Patch Update advisory to reduce exposure in the interim, which may include restricting or blocking the network protocols required for the attack at the network edge. Treat any such workaround as a temporary risk-reduction measure only, test changes on non-production systems first to avoid breaking application functionality, and complete full patching as soon as possible because a workaround does not correct the underlying flaw.

**Hunt for Signs of Exploitation:** Review web server and proxy logs for anomalous or specially crafted HTTP requests directed at the WebLogic Server Proxy Plug-in, and investigate any evidence of unexpected data creation, deletion, or modification on affected servers. Because exploitation attempts have been observed since shortly after public proof-of-concept release, retrospective log review across the exposure window is warranted, and any confirmed compromise should be escalated to incident response for containment and forensic analysis.

**Strengthen Vulnerability and Asset Management:** Maintain an accurate, continuously updated inventory of Oracle Fusion Middleware components, including WebLogic Server Proxy Plug-in and Oracle HTTP Server versions, so that affected assets can be located rapidly when advisories are published. Integrate authoritative feeds into vulnerability prioritization, enforce timely patch cycles for internet-facing middleware, and reduce the external attack surface by ensuring management and proxy interfaces are not needlessly exposed to untrusted networks.

# Potential MITRE ATT&CK TTPs

| Tactic | Technique | Sub-technique |
|---|---|---|
| Initial Access | T1190: Exploit Public-Facing Application | |
| Reconnaissance | T1595: Active Scanning | T1595.002: Vulnerability Scanning |
| Resource Development | T1588: Obtain Capabilities | T1588.006: Vulnerabilities |

## Patch Links

https://www.oracle.com/security-alerts/cpujan2026.html

## References

https://www.oracle.com/security-alerts/cpujan2026.html

https://arcticwolf.com/resources/blog/cve-2026-21962/

https://www.caloes.ca.gov/wp-content/uploads/Cal-CSIC-Cyber-Advisory-Oracle-Weblogic-Server-Proxy-Plug-in-product-of-Oracle-Fusion-Middleware-Vulnerability.pdf

https://github.com/gregk4sec/CVE-2026-21962

# 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 Demo of **HivePro**.

REPORT GENERATED ON

**August 26, 2026 • 07:30 AM**



More at www.hivepro.com