

Alert Bulletin

Bulletin N.:

Publication Date: 25/08/2026

Subject: Security update: Critical RCE in Oracle WebLogic actively exploited

Traffic Light Protocol (TLP): White

CISA has once again added CVE-2026-21962 to its catalog of actively exploited vulnerabilities, confirming attacks against vulnerable instances of Oracle HTTP Server and Oracle WebLogic Server Proxy Plug-in. The flaw, with critical severity (CVSS 10.0), allows a remote and unauthenticated attacker to leverage an improper access control to obtain unauthorized access to critical information via HTTP.

Organizations using the affected versions—12.2.1.4.0, 14.1.1.0.0, and 14.1.2.0.0—should treat this situation as a priority: apply the patch published by Oracle in its January 2026 update, limit the external exposure of services while remediation is completed, and review logs to identify potential anomalous accesses or requests.

Affected product(s):

The affected components include:

- Versions of Oracle HTTP Server and Oracle WebLogic Server Proxy Plug-in (Apache):
 - o 12.2.1.4.0
 - o 14.1.1.0.0
 - o 14.1.2.0.0
- Oracle WebLogic Server Proxy Plug-in for IIS version 12.2.1.4.0

Description

A critical unauthenticated vulnerability has been reported affecting Oracle HTTP Server and the Oracle WebLogic Server Proxy Plug-in for Apache and IIS. By sending specially crafted HTTP requests, a remote attacker can compromise the proxy component without authentication. It has been identified as CVE-2026-21962 with a CVSSv3 score of 10.

A successful exploitation can result in unauthorized access to confidential data and the ability to create, modify, or delete data processed by the proxy and, potentially, by subsequent applications, which represents a significant risk for enterprise environments, especially implementations connected to the internet.

Mitigation

- Restrict the network exposure of proxy server and HTTP components by placing them behind firewalls, WAF, or VPN/ZTNA solutions, and allow access only from trusted networks.
- Review web and proxy logs to detect suspicious request patterns, unexpected endpoints, or abnormal data access activity.

Solution

Immediately apply the Oracle critical patch update from January 2026 to all affected installations of Oracle HTTP Server and WebLogic Proxy Plug-in, prioritizing internet-connected systems.

At the following link you can find information on how to proceed with the update of your system:

<https://support.oracle.com/support/?documentId=KA1396>

<https://www.oracle.com/security-alerts/cpujan2026.html#AppendixFMW>

Additional information:

- <https://www.redlegg.com/blog/security-bulletin-oracle-proxy-components-vulnerable-to-unauthenticated-attack>
- <https://www.oracle.com/security-alerts/cpujan2026.html>