An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre

NCSC #2601230201

NCSC Advisory

Oracle Corporation: Oracle HTTP Server, Oracle Weblogic Server Proxy Plug-in

CVE-2026-21962

23rd, January 2026

STATUS: TLP:CLEAR

Recipients can spread this to the world, there is no limit on disclosure. Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.

For more information on the Traffic Light Protocol, see https://www.first.org/tlp/. Please treat this document in accordance with the TLP assigned.

Description

CVE ID: CVE-2026-21962

Published: 2026-01-20

Vendor: Oracle Corporation

Product: Oracle HTTP Server, Oracle Weblogic Server Proxy Plug-in

CVSS Score[1]: 10

CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:N)

Products Affected

Product	Version
Oracle HTTP Server, Oracle Weblogic Server Proxy Plug-in	12.2.1.4.0
Oracle HTTP Server, Oracle Weblogic Server Proxy Plug-in	14.1.1.0.0
Oracle HTTP Server, Oracle Weblogic Server Proxy Plug-in	14.1.2.0.0

Impact

Vulnerability in the Oracle HTTP Server, Oracle Weblogic Server Proxy Plug-in product of Oracle Fusion Middleware (component: Weblogic Server Proxy Plug-in for Apache HTTP Server, Weblogic Server Proxy Plug-in for IIS).

This easily exploitable vulnerability allows an unauthenticated attacker with network access via HTTP to compromise Oracle HTTP Server, Oracle Weblogic Server Proxy Plug-in. While the vulnerability is in Oracle HTTP Server, Oracle Weblogic Server Proxy Plug-in, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle HTTP Server, Oracle Weblogic Server Proxy Plug-in accessible data as well as unauthorized access to critical data or complete access to all Oracle HTTP Server, Oracle Weblogic Server Proxy Plug-in accessible data.

Note: Affected version for Weblogic Server Proxy Plug-in for IIS is 12.2.1.4.0 only.

Oracle reports that it has reports of attempts to exploit the vulnerability.

[1] https://www.first.org/cvss/

Common Weakness Enumeration (CWE)[2]: CWE-284: Improper Access Control

Known Exploited Vulnerability (KEV) catalog[3]: No

Used by Ransomware Operators: N/A

Recommendations

The NCSC strongly recommends -

- Patching affected Oracle WebLogic systems for CVE-2026-21962 **immediately**
- Monitoring HTTP traffic for suspicious behaviour
- Reviewing system logs and security controls

The NCSC strongly recommends installing updates for vulnerable systems with the highest priority, after thorough testing. Affected organisations should review the latest release notes and install the relevant updates from Oracle Corporation.

- https://nvd.nist.gov/vuln/detail/CVE-2026-21962
- https://www.cve.org/CVERecord?id=CVE-2026-21962
- https://www.oracle.com/security-alerts/cpujan2026.html
- https://github.com/Ashwesker/Ashwesker-CVE-2026-21962

[2] https://cwe.mitre.org
[3] https://www.cisa.gov/known-exploited-vulnerabilities-catalog