

CVE-2026-21962

Oracle HTTP Server and Oracle Weblogic Server Proxy Plug-in Improper Access Control Vulnerability

CISA KEV since Aug 24, 2026

Actively exploited

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). Supported versions that are affected are 12.2.1.4.0, 14.1.1.0.0 and 14.1.2.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle HTTP Server, Oracle Weblogic Server Proxy Plug-in.

EVRS

85/100

Immediate priority

CVSS V3.1

10.0

Critical · NVD

EPSS

0.732

99.46th percentile · FIRST

CISA DEADLINE

Aug 27, 2026

CISA federal deadline · Overdue by 56 days

Signals behind the score

☒ counted in the score ☐ not counted

evidence for 6 of 8 signals

☒ CISA KEV	Listed in the catalog	☐ Vendor exploitation	Confirmed exploitation in the wild
☐ Ransomware	No known ransomware campaign association	☒ KEV recency	Added to CISA KEV within the last 90 days
☒ EPSS	0.732 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 10.0	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch Immediately Patch or fixed version identified

CISA required action: Apply mitigations in accordance with vendor instructions, ensuring compliance with CISA's BOD 26-04 Prioritizing Security Updates Based on Risk (see URL in Notes) guidance and CISA's "Forensics Triage Requirements" (see URL in Notes). Follow applicable BOD 26-04 guidance for cloud services or discontinue use of the product if mitigations are unavailable. Stakeholders are responsible for evaluating each asset's internet exposure and ensuring adherence to BOD 26-04 patching guidelines.

Basis: CISA KEV required action

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. CVSS 3.1 Base Score 10.0 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:N).

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
http server	12.2.1.4.0	no fixed version listed	NVD
	14.1.1.0.0		
	14.1.2.0.0		
weblogic server proxy plug-in	12.2.1.4.0	no fixed version listed	NVD
	14.1.1.0.0		
	14.1.2.0.0		



Sources

Vendor guidance	oracle.com/security-alerts/cpujan2026.html	BOD 26-04	cisa.gov/news-events/directives/bod-26-04-prioritizing-security-updates-based-risk
Forensics Triage Requirements	cisa.gov/news-events/directives/bod-26-04-implementation-guidance-prioritizing-security-updates-based-risk	NVD	nvd.nist.gov/vuln/detail/CVE-2026-21962
CISA KEY	cisa.gov/known-exploited-vulnerabilities-catalog	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2026-3550
Current data	evulnable.com/vulnerability-management/cve/CVE-2026-21962		

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.