EXPLOITED VULNERABILITY ADVISORY: CVE-2026-21962

Summary

CVE-2026-21962 in Oracle HTTP Server and Oracle Weblogic Server Proxy Plug-in is being actively exploited in the wild. 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. 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). CISA requires federal remediation by 2026-08-27; under the CRA, exploitation of an affected product must be reported within 24 hours.

What we know

- **CVE:** CVE-2026-21962
- **Affected:** Oracle HTTP Server and Oracle Weblogic Server Proxy Plug-in
- **Exploitation:** Actively exploited, added to CISA KEV on 2026-08-24
- **Severity:** CVSS 10.0 Critical, Network-exploitable, no privileges required, no user interaction (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:N)
- **Exploitation likelihood (EPSS):** 43%
- **Weakness:** CWE-284

Recommended action

Patch CVE-2026-21962 by 2026-08-27. If you cannot patch immediately, restrict network access to the affected service now (segment it, put it behind a VPN, or take it offline) until you can patch. If you ship an affected product, be ready to file the CRA 24-hour report the moment you find it exploited.

Sources: CISA Known Exploited Vulnerabilities, NIST NVD. Public data; an advisory of active exploitation, not an incident report. Verify applicability to your estate before acting.