CYBER ADVISORY

Thursday, January 22, 2026

CSIC-ADVISORY-202601-A-007

Critical Vulnerability in Oracle HTTP Server, Oracle WebLogic Server Proxy Plug-in

Data Creation and Deletion	Crafted HTTP Requests	Patch Available	Data Modification

The California Cybersecurity Integration Center (Cal-CSIC) has identified a critical vulnerability impacting Oracle HTTP Server, Oracle WebLogic Server Proxy Plug-in. CVE-2026-21962 carries a CVSS 3.1 score of 10.0.[1] Successful exploitation of this vulnerability grants an unauthenticated attacker unauthorized creation, deletion, and modification access to Oracle HTTP Server and WebLogic Server Proxy Plug-in data via specially crafted HTTP requests. The attacker can create, delete, or modify any data accessible to the web server, greatly compromising the integrity and confidentiality of the entire server.[2] CVE-2026-21962 is not currently known to be exploited in the wild or as a zero-day. The vendor has issued a critical patch update advisory with patching and workaround instructions.

The Cal-CSIC recommends immediately following the vendor's guidance in mitigation and remediation, to include immediate patching. If immediate patching is delayed, please follow the vendor's guidance for workarounds.[3]

For further information on Oracle's critical patch update advisory please use this link:

Security Advisory

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

Affected Product:

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

References

[1] NVD; “CVE-2026-21962”; https://www.cvedetails.com/cve/CVE-2025-65037/; accessed 21 January 2026
[2] Tenable; “CVE-2026-21962”; https://www.tenable.com/cve/CVE-2026-21962; accessed 21 January 2026
[3] Oracle; “Oracle Critical Patch Update Advisory – January 2026”; https://www.oracle.com/security-alerts/cpujan2026.html; accessed 21 January 2026