CYBER ADVISORY

Thursday, January 22, 2026

CSIC-ADVISORY-202601-A-008

Critical Vulnerability in Oracle Agile Product Lifecycle Management Process

Unauthorized Access	Compromised Integrity	Patch Available	Compromised Confidentiality

The California Cybersecurity Integration Center (Cal-CSIC) has identified a critical vulnerability impacting Oracle's Agile Product Lifecycle Management (PLM) for Process product within Oracle's Supplier Portal component. CVE-2026-21969 carries a CVSS 3.1 score of 9.8.[1] Successful exploitation of this vulnerability allows a remote attacker to obtain unauthorized access via HTTP.[2] Compromise of the Oracle Agile PLM would threaten the confidentiality by having access to supplier and product data as well as its integrity by altering, deleting, or creating unauthorized data within the system.

CVE-2026-21969 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.[3]

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.

For further information on Oracle's Critical Patch Update Advisory please use this link:

Security Advisory

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

Affected Product:

Product	Affected Version
Oracle Agile Product Lifecycle Management for Process	6.2.4

References

[1] NVD; “CVE-2026-21969”; https://nvd.nist.gov/vuln/detail/CVE-2026-21969; accessed 21 January 2026
[2] Tenable; “CVE-2026-21969”; https://www.tenable.com/cve/CVE-2026-21969; accessed 21 January 2026
[3] Oracle; “Oracle Critical Patch Update Advisory – January 2026”; https://www.oracle.com/security-alerts/cpujan2026.html#AppendixSCP; accessed 21 January 2026