

Alert Bulletin

Bulletin N.: 106

Publication Date: 21/09/2026

Subject: Alert 2026-106 RCE in Oracle WebLogic Server — CVE~~2026~~70757

Traffic Light Protocol (TLP): White

Affected product(s):

Oracle identifies these supported versions as affected:

Product	Component	Affected versions
Oracle WebLogic Server	Core	12.2.1.4.0
Oracle WebLogic Server	Core	14.1.1.0.0
Oracle WebLogic Server	Core	14.1.2.0.0
Oracle WebLogic Server	Core	15.1.1.0.0

The exact patch availability, *patch* number, and prerequisites must be confirmed in **My Oracle Support (MOS)**, using the September 2026 Critical Patch Update and the patch matrix corresponding to the environment.

Description

A critical vulnerability was identified in the **Core** component of Oracle WebLogic Server, part of Oracle Fusion Middleware. The flaw has a **CVSS 9.8 score, identified as CVE 2026 70757** and allows an unauthenticated remote attacker, with network access to the **T3** or **IIOP** protocols, to fully compromise a vulnerable WebLogic Server instance.

The vulnerability was fixed as part of the **September 2026 Oracle Critical Patch Update (CPU)**. No authentication, user interaction, or complex exploitation conditions are required; therefore, WebLogic servers that have T3, IIOP, administrative consoles, or applications exposed to the Internet or accessible from untrusted networks should be prioritized.

Solution

The definitive remediation consists of applying the corresponding patch from the **September 2026 Oracle Critical Patch Update** for CVE~~2026~~70757. Patch downloads and detailed installation steps are available for

authorized customers through **My Oracle Support**.

<https://support.oracle.com/signin>

No mitigation is identified that completely eliminates the vulnerability. Blocking T3/ILOP, disabling unused ILOP, and connection filters temporarily reduce the attack surface, but do not replace the official patch.

After updating, validate that:

1. The WebLogic domain inventory has the patch applied.
2. T3/ILOP ports are only available to authorized sources.
3. The administrative console is not directly exposed to the Internet.
4. Applications and *datasources* operate correctly after the restart.
5. Unauthorized changes and possible signs of prior exploitation have been reviewed.

Additional information:

- <https://www.oracle.com/security-alerts/cspusep2026.html>
- <https://www.oracle.com/security-alerts/cspusep2026verbose.html>
- <https://nvd.nist.gov/vuln/detail/CVE-2026-70757>
- <https://www.ionix.io/threat-center/cve-2026-70757/>