CVE-2020-2883

Oracle WebLogic Server Unspecified Vulnerability

Exigent | CISA KEV since Jan 7, 2025 | Actively exploited | Public exploit module (Metasploit)

Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0 and 12.2.1.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via IIOP, T3 to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server. CVSS 3.0 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).

EVRS	CVSS V3.1	EPSS	CISA DEADLINE
87/100 Immediate priority	9.8 Critical · NVD	0.946 99.86th percentile · FIRST	Jan 28, 2025 KEV since 2025 · listed over a year

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 two years
✓ EPSS	0.946 probability	− Pre-patch disclosure	Disclosure status unavailable
✓ CVSS	Base score 9.8	− Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Out-of-band / urgent — Patch or fixed version identified

CISA required action: Apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable.

Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
weblogic server	10.3.6.0.0 12.1.3.0.0 12.2.1.3.0 12.2.1.4.0	no fixed version listed	NVD

Sources

Vendor guidance	github.com/advisories/GHSA-9x8q-p3qp-r24w	Additional guidance	oracle.com/security-alerts/cpuapr2020.html
NVD	nvd.nist.gov/vuln/detail/CVE-2020-2883	CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog
ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2020-22676	Current data	evulnable.com/vulnerability-management/cve/CVE-2020-2883

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