



# CVE-2020-6950

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2020-6950
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2021-06-02 16:15:00 UTC
<b>Updated</b>	2022-05-12 14:06:00 UTC
<b>Description</b>	Directory traversal in Eclipse Mojarra before 2.3.14 allows attackers to read arbitrary files via the loc parameter or con para

## Risk And Classification

### Problem Types: CWE-22

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Eclipse</a>	<a href="#">Mojarra</a>	All	All	All	All
Application	<a href="#">Oracle</a>	<a href="#">Banking Enterprise Default Management</a>	2.10.0	All	All	All
Application	<a href="#">Oracle</a>	<a href="#">Banking Enterprise Default Management</a>	2.12.0	All	All	All
Application	<a href="#">Oracle</a>	<a href="#">Banking Platform</a>	2.12.0	All	All	All
Application	<a href="#">Oracle</a>	<a href="#">Banking Platform</a>	2.6.2	All	All	All
Application	<a href="#">Oracle</a>	<a href="#">Banking Platform</a>	2.7.1	All	All	All
Application	<a href="#">Oracle</a>	<a href="#">Banking Platform</a>	2.9.0	All	All	All
Application	<a href="#">Oracle</a>	<a href="#">Communications Network Integrity</a>	7.3.6	All	All	All
Application	<a href="#">Oracle</a>	<a href="#">Communications Pricing Design Center</a>	12.0.0.3.0	All	All	All
Application	<a href="#">Oracle</a>	<a href="#">Hyperion Calculation Manager</a>	All	All	All	All
Application	<a href="#">Oracle</a>	<a href="#">Retail Merchandising System</a>	19.0.1	All	All	All
Application	<a href="#">Oracle</a>	<a href="#">Solaris Cluster</a>	4.0	All	All	All
Application	<a href="#">Oracle</a>	<a href="#">Time And Labor</a>	All	All	All	All

## References

Reference	Source	Link	Tags
550943 – Mojarra multiple directory traversal issues	MISC	<a href="https://bugs.eclipse.org">bugs.eclipse.org</a>	

Oracle Critical Patch Update Advisory - April 2022	MISC	<a href="http://www.oracle.com">www.oracle.com</a>	
Multiple Path Traversal security issues · Issue #4571 · eclipse-ee4j/mojarra · GitHub	MISC	<a href="https://github.com">github.com</a>	
Oracle Critical Patch Update Advisory - October 2021	MISC	<a href="http://www.oracle.com">www.oracle.com</a>	
Oracle Critical Patch Update Advisory - January 2022	MISC	<a href="http://www.oracle.com">www.oracle.com</a>	
Multiple Path Traversal security issues · eclipse-ee4j/mojarra@cefb94 · GitHub	MISC	<a href="https://github.com">github.com</a>	
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>	canonical, analysis

No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

[150676](#) Oracle WebLogic Server Multiple Vulnerabilities (APR-2023)

[690471](#) Free Berkeley Software Distribution (FreeBSD) Security Update for payara (b07bdd3c-0809-11eb-a3a4-0019dbb15b3f)

[87542](#) Oracle WebLogic Server Multiple Vulnerabilities (CPUAPR2023)

[980356](#) Java (maven) Security Update for org.glassfish:mojarra-parent (GHSA-rpq8-mmwh-q9hm)

© [CVE.report](https://cve.report) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](#).

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)