



# CVE-2019-17566

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

## Summary

<b>CVE</b>	CVE-2019-17566
<b>State</b>	PUBLIC
<b>Assigner</b>	security@apache.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2020-11-12 18:15:00 UTC
<b>Updated</b>	2024-01-07 11:15:00 UTC
<b>Description</b>	Apache Batik is vulnerable to server-side request forgery, caused by improper input validation by the "xlink:href" attributes.

## Risk And Classification

**Problem Types:** CWE-918

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Apache</a>	<a href="#">Batik</a>	All	All	All	All
Application	<a href="#">Apache</a>	<a href="#">Batik</a>	All	All	All	All
Application	<a href="#">Oracle</a>	<a href="#">Api Gateway</a>	11.1.2.4.0	All	All	All
Application	<a href="#">Oracle</a>	<a href="#">Business Intelligence</a>	12.2.1.3.0	All	All	All
Application	<a href="#">Oracle</a>	<a href="#">Business Intelligence</a>	12.2.1.4.0	All	All	All
Application	<a href="#">Oracle</a>	<a href="#">Business Intelligence</a>	5.5.0.0.0	All	All	All
Application	<a href="#">Oracle</a>	<a href="#">Business Intelligence</a>	5.9.0.0.0	All	All	All
Application	<a href="#">Oracle</a>	<a href="#">Communications Application Session Controller</a>	3.9m0p2	All	All	All
Application	<a href="#">Oracle</a>	<a href="#">Communications Metasolv Solution</a>	All	All	All	All
Application	<a href="#">Oracle</a>	<a href="#">Communications Offline Mediation Controller</a>	12.0.0.3.0	All	All	All
Application	<a href="#">Oracle</a>	<a href="#">Enterprise Repository</a>	11.1.1.7.0	All	All	All
Application	<a href="#">Oracle</a>	<a href="#">Financial Services Analytical Applications Infrastructure</a>	All	All	All	All
Application	<a href="#">Oracle</a>	<a href="#">Fusion Middleware Mapviewer</a>	12.2.1.4.0	All	All	All
Application	<a href="#">Oracle</a>	<a href="#">Hospitality Opera 5</a>	5.5	All	All	All
Application	<a href="#">Oracle</a>	<a href="#">Hospitality Opera 5</a>	5.6	All	All	All
Application	<a href="#">Oracle</a>	<a href="#">Hyperion Financial Reporting</a>	11.1.2.4	All	All	All
Application	<a href="#">Oracle</a>	<a href="#">Hyperion Financial Reporting</a>	11.2.5.0	All	All	All

Application	Oracle	Instantis Enterprisetrack	All	All	All	All
Application	Oracle	Jd Edwards Enterpriseone Tools	All	All	All	All
Application	Oracle	Jd Edwards Enterpriseone Tools	9.2.4.2	All	All	All
Application	Oracle	Retail Integration Bus	15.0.3	All	All	All
Application	Oracle	Retail Order Broker	15.0	All	All	All
Application	Oracle	Retail Order Broker	16.0	All	All	All
Application	Oracle	Retail Order Management System Cloud Service	19.5	All	All	All
Application	Oracle	Retail Point-of-service	14.1	All	All	All
Application	Oracle	Retail Returns Management	14.1	All	All	All

## References

Reference	Source
Pony Mail!	MLIST
[myfaces-commits] 20201211 [myfaces-tobago] 21/22: Update batik dependency from 1.9 to 1.13, because of CVE-2019-17566	MLIST
Oracle Critical Patch Update Advisory - July 2021	N/A
GLSA-202401-11	
Oracle Critical Patch Update Advisory - October 2021	MISC
Oracle Critical Patch Update Advisory - January 2022	MISC
Pony Mail!	
Pony Mail!	
The Apache(tm) XML Graphics Project - Community	MISC
Oracle Critical Patch Update Advisory - July 2022	N/A
Oracle Critical Patch Update Advisory - April 2021	MISC
Oracle Critical Patch Update Advisory - January 2021	MISC
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

<a href="#">199377</a> Ubuntu Security Notification for Apache Batik Vulnerabilities (USN-6117-1)
<a href="#">710829</a> Gentoo Linux Apache Batik Multiple Vulnerabilities (GLSA 202401-11)
<a href="#">755916</a> SUSE Enterprise Linux Security Update for xmlgraphics-batik (SUSE-SU-2024:0777-1)
<a href="#">87496</a> Oracle WebLogic Server Multiple Vulnerabilities (CPUJUL2022)

---

© [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](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**CVE.report and Source URL Uptime Status [status.cve.report](#)**