



CVE-2016-0779

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

Summary

CVE	CVE-2016-0779
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-04-11 16:59:00 UTC
Updated	2018-10-09 19:58:00 UTC
Description	The EjbObjectInputStream class in Apache TomEE before 1.7.4 and 7.x before 7.0.0-M3 allows remote attackers to execut

Risk And Classification

Problem Types: CWE-502

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apache	Tomee	7.0.0	m1	All	All
Application	Apache	Tomee	7.0.0	m1	All	All
Application	Apache	Tomee	All	All	All	All

References

Reference	Source	Link	Tags
Apache TomEE	CONFIRM	tomee.apache.org	Patch,
Zero Day Initiative	MISC	www.zerodayinitiative.com	Third F
SecurityFocus	BUGTRAQ	www.securityfocus.com	
TomEE Dev - Document resolved vulnerability CVE-2015-8581	MLIST	tomee-openejb.979440.n4.nabble.com	Issue
Apache TomEE Patched ~ Packet Storm	MISC	packetstormsecurity.com	Third F
Apache TomEE 'EjbObjectInputStream' Remote Code Execution Vulnerability	BID	www.securityfocus.com	Third F
CVE Program record	CVE.ORG	www.cve.org	canoni
NVD vulnerability detail	NVD	nvd.nist.gov	canoni

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [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](#)