



CVE-2018-1048

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

Summary

CVE	CVE-2018-1048
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-01-24 23:29:00 UTC
Updated	2023-02-03 02:19:00 UTC
Description	It was found that the AJP connector in undertow, as shipped in Jboss EAP 7.1.0.GA, does not use the ALLOW_ENCODED

Risk And Classification

Problem Types: CWE-22 | CWE-116

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Redhat	Jboss Enterprise Application Platform	7.1.0	All	All	All
Application	Redhat	Jboss Enterprise Application Platform	7.1.0	All	All	All

References

Reference
Red Hat Customer Portal
Red Hat Customer Portal
Red Hat Customer Portal
1534343 – (CVE-2018-1048) CVE-2018-1048 undertow: ALLOW_ENCODED_SLASH option not taken into account in the AjpRequestParser
Red Hat Customer Portal
CVE Program record
NVD vulnerability detail

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](#).

Free CVE JSON API [cve.report/api](#)

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