



CVE-2022-2053

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

Summary

CVE	CVE-2022-2053
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-08-05 16:15:00 UTC
Updated	2022-08-11 14:06:00 UTC
Description	When a POST request comes through AJP and the request exceeds the max-post-size limit (maxEntitySize), Undertow's A

Risk And Classification

Problem Types: CWE-400

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Redhat	Integration Camel K	-	All	All	All
Application	Redhat	Jboss Fuse	7.0.0	All	All	All
Application	Redhat	Undertow	All	All	All	All
Application	Redhat	Undertow	2.3.0	alpha1	All	All

References

Reference	Source	Link	Tags
2095862 – (CVE-2022-2053) CVE-2022-2053 undertow: Large AJP request may cause DoS	MISC	bugzilla.redhat.com	
[UNDERTOW-2133] CVE-2022-2053: Large AJP request may cause DoS - Red Hat Issue Tracker	MISC	issues.redhat.com	
CVE Program record	CVE.ORG	www.cve.org	cano
NVD vulnerability detail	NVD	nvd.nist.gov	cano

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[240711](#) Red Hat Update for JBoss Enterprise Application Platform 7.4.7 (RHSA-2022:6822)

[240712](#) Red Hat Update for JBoss Enterprise Application Platform 7.4.7 (RHSA-2022:6823)

© [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](#)