



CVE-2021-3642

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2021-3642
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-08-05 21:15:00 UTC
Updated	2021-10-20 14:36:00 UTC
Description	A flaw was found in Wildfly Elytron in versions prior to 1.10.14.Final, prior to 1.15.5.Final and prior to 1.16.1.Final where ScramServer

Risk And Classification

Problem Types: CWE-203

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Quarkus	Quarkus	All	All	All	All
Application	Redhat	Build Of Quarkus	-	All	All	All
Application	Redhat	Codeready Studio	12.0	All	All	All
Application	Redhat	Data Grid	8.0	All	All	All
Application	Redhat	Descision Manager	7.0	All	All	All
Application	Redhat	Integration Camel K	-	All	All	All
Application	Redhat	Integration Camel Quarkus	All	All	All	All
Application	Redhat	Jboss Enterprise Application Platform	7.0.0	All	All	All
Application	Redhat	Jboss Enterprise Application Platform Expansion Pack	-	All	All	All
Application	Redhat	Jboss Fuse	7.0.0	All	All	All
Application	Redhat	Openshift Application Runtimes	-	All	All	All
Application	Redhat	Process Automation	7.0	All	All	All
Application	Redhat	Wildfly Elytron	All	All	All	All

References

Reference	Source	Link	Tags
1981407 – (CVE-2021-3642) CVE-2021-3642 wildfly-elytron: possible timing attack in ScramServer	MISC	bugzilla.redhat.com	

CVE Program record	CVE.ORG	www.cve.org	canc
NVD vulnerability detail	NVD	nvd.nist.gov	canc

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[239652](#) Red Hat Update for Red Hat JBoss Enterprise Application Platform 7.4.1 (RHSA-2021:3658)

[239653](#) Red Hat Update for Red Hat JBoss Enterprise Application Platform 7.4.1 (RHSA-2021:3656)

[239965](#) Red Hat Update for JBoss Enterprise Application Platform 7.3.10 on RHEL 7 (RHSA-2021:5150)

[239966](#) Red Hat Update for JBoss Enterprise Application Platform 7.3.10 on RHEL 8 (RHSA-2021:5151)

[239967](#) Red Hat Update for JBoss Enterprise Application Platform 7.3.10 on RHEL 6 (RHSA-2021:5149)

© [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](#)