



CVE-2019-14887

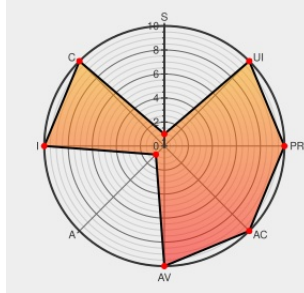
Published on: 03/16/2020 12:00:00 AM UTC

Last Modified on: 02/12/2023 11:06:59 PM UTC

CVE-2019-14887

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

CVSS:31/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N



Certain versions of [Jboss Data Grid](#) from [Redhat](#) contain the following vulnerability:

A flaw was found when an OpenSSL security provider is used with Wildfly, the 'enabled-protocols' value in the Wildfly configuration isn't honored. An attacker could target the traffic sent from Wildfly and downgrade the connection to a weaker version of TLS, potentially breaking the encryption. This could lead to a leak of the data being passed over the network. Wildfly version 7.2.0.GA, 7.2.3.GA and 7.2.5.CR2 are believed to be vulnerable.

CVE-2019-14887 has been assigned by [secalert@redhat.com](#) to track the vulnerability - currently rated as **CRITICAL** severity.

Affected Vendor/Software: **Red Hat** - **wildfly** version = **7.2.0.GA, 7.2.3.GA, 7.2.5.CR2**

CVSS3 Score: **9.1 - CRITICAL**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	NONE

CVSS2 Score: **6.4 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	NONE

CVE References

Description	Tags	Link
1772008 – (CVE-2019-14887) CVE-2019-14887 wildfly: The 'enabled-protocols' value in legacy security is not respected if OpenSSL security provider is in use	Issue Tracking Vendor Advisory bugzilla.redhat.com text/html	 CONFIRM bugzilla.redhat.com/show_bug.cgi?id=CVE-2019-14887
Login server redirect	Permissions Required issues.redhat.com text/html	 CONFIRM issues.redhat.com/browse/JBEAP-17965
CVE-2019-14887 Wildfly Vulnerability in NetApp Products NetApp Product Security	security.netapp.com text/html	 CONFIRM security.netapp.com/advisory/ntap-20200327-0007/

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Redhat	Jboss Data Grid	7.0.0	All	All	All
Application	Redhat	Jboss Data Grid	7.0.0	All	All	All
Application	Redhat	Jboss Enterprise Application Platform	7.0.0	All	All	All
Application	Redhat	Jboss Enterprise Application Platform	7.0.0	All	All	All
Application	Redhat	Jboss Fuse	7.0.0	All	All	All
Application	Redhat	Jboss Fuse	7.0.0	All	All	All
Application	Redhat	Openshift Application Runtimes	-	All	All	All
Application	Redhat	Openshift Application Runtimes	-	All	All	All
Application	Redhat	Single Sign-on	7.0	All	All	All
Application	Redhat	Single Sign-on	7.0	All	All	All
Application	Redhat	Wildfly	7.2.0	general_availability	All	All
Application	Redhat	Wildfly	7.2.3	general_availability	All	All
Application	Redhat	Wildfly	7.2.5	cr2	All	All
Application	Redhat	Wildfly	7.2.0	general_availability	All	All
Application	Redhat	Wildfly	7.2.3	general_availability	All	All
Application	Redhat	Wildfly	7.2.5	cr2	All	All

cpe:2.3:a:redhat:jboss_data_grid:7.0.0:*:*:*:*:*:

cpe:2.3:a:redhat:jboss_data_grid:7.0.0:*:*:*:*:*:

cpe:2.3:a:redhat:jboss_enterprise_application_platform:7.0.0:*:*:*:*:*:

cpe:2.3:a:redhat:jboss_enterprise_application_platform:7.0.0:*:*:*:*:*:
cpe:2.3:a:redhat:jboss_fuse:7.0.0:*:*:*:*:*:
cpe:2.3:a:redhat:jboss_fuse:7.0.0:*:*:*:*:*:
cpe:2.3:a:redhat:openshift_application_runtimes:*:*:*:*:*:
cpe:2.3:a:redhat:openshift_application_runtimes:*:*:*:*:*:
cpe:2.3:a:redhat:single_sign-on:7.0:*:*:*:*:*:
cpe:2.3:a:redhat:single_sign-on:7.0:*:*:*:*:*:
cpe:2.3:a:redhat:wildfly:7.2.0:general_availability:*:*:*:*:*:
cpe:2.3:a:redhat:wildfly:7.2.3:general_availability:*:*:*:*:*:
cpe:2.3:a:redhat:wildfly:7.2.5:cr2:*:*:*:*:*:
cpe:2.3:a:redhat:wildfly:7.2.0:general_availability:*:*:*:*:*:
cpe:2.3:a:redhat:wildfly:7.2.3:general_availability:*:*:*:*:*:
cpe:2.3:a:redhat:wildfly:7.2.5:cr2:*:*:*:*:*:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)