



CVE-2018-14627

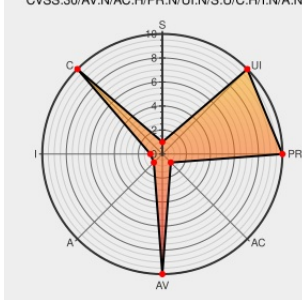
Published on: 09/04/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:44 PM UTC

CVE-2018-14627

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

CVSS:30/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N



Certain versions of [Wildfly](#) from [Redhat](#) contain the following vulnerability:

The IOP OpenJDK Subsystem in WildFly before version 14.0.0 does not honour configuration when SSL transport is required. Servers before this version that are configured with the following setting allow clients to create plaintext connections: `<transport-config confidentiality="required" trust-in-target="supported"/>`

CVE-2018-14627 has been assigned by [secalert@redhat.com](#) to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: **[UNKNOWN]** - **JBoss/WildFly** version **14.0.0**

CVSS3 Score: **5.9 - MEDIUM**

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

CVSS2 Score: **4.3 - MEDIUM**

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

CVE References

Description	Tags	Link
-------------	------	------

Red Hat Customer Portal	Third Party Advisory access.redhat.com text/html	 REDHAT RHSA-2018:3528
Red Hat Customer Portal	Third Party Advisory access.redhat.com text/html	 REDHAT RHSA-2018:3529
[WFLY-9107] Block non-SSL IIOP port when SSL transport is required - Red Hat Issue Tracker	Third Party Advisory issues.jboss.org text/html	 CONFIRM issues.jboss.org/browse/WFLY-9107
1624664 – (CVE-2018-14627) CVE-2018-14627 JBoss/WildFly: iiop does not honour strict transport confidentiality	Issue Tracking Patch Third Party Advisory bugzilla.redhat.com text/html	 CONFIRM bugzilla.redhat.com/show_bug.cgi?id=CVE-2018-14627
CVE-2018-14627 Wildfly Vulnerability in NetApp Products NetApp Product Security	security.netapp.com text/html	 CONFIRM security.netapp.com/advisory/ntap-20181221-0002/
Red Hat Customer Portal	Third Party Advisory access.redhat.com text/html	 REDHAT RHSA-2018:3527
Red Hat Customer Portal	Third Party Advisory access.redhat.com text/html	 REDHAT RHSA-2018:3595

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	Wildfly	All	All	All	All
Application	Redhat	Wildfly	All	All	All	All
cpe:2.3:a:redhat:wildfly:*****:*****:*						
cpe:2.3:a:redhat:wildfly:*****:*****:*						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

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](#)