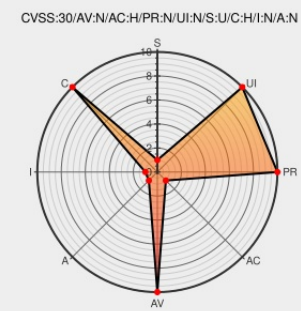
CVE-2017-12196

Published on: 04/17/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:29 PM UTC

CVE-2017-12196

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Jboss Enterprise Application Platform from Redhat contain the following vulnerability:

undertow before versions 1.4.18.SP1, 2.0.2.Final, 1.4.24.Final was found vulnerable when using Digest authentication, the server does not ensure that the value of URI in the Authorization header matches the URI in HTTP request line. This allows the attacker to cause a MITM attack and access the desired content on the server.

CVE-2017-12196 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as MEDIUM severity.

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
[UNDERTOW-1190] client can use bogus uri in digest authentication - Red Hat Issue Tracker	Issue Tracking, issues.jboss.org, text/html	CONFIRM issues.jboss.org/browse/UNDERTOW-1190

Red Hat Customer Portal	Vendor Advisory access.redhat.com text/html	REDHAT RHSA-2018:0481
Red Hat Customer Portal	Vendor Advisory access.redhat.com text/html	REDHAT RHSA-2018:2405
Red Hat Customer Portal	Vendor Advisory access.redhat.com text/html	REDHAT RHSA-2018:0480
Red Hat Customer Portal	Vendor Advisory access.redhat.com text/html	REDHAT RHSA-2018:3768
Red Hat Customer Portal	Vendor Advisory access.redhat.com text/html	REDHAT RHSA-2018:0479
Red Hat Customer Portal	Vendor Advisory access.redhat.com text/html	REDHAT RHSA-2018:1525
1503055 – (CVE-2017-12196) CVE-2017-12196 undertow: Client can use bogus uri in Digest authentication	Issue Tracking Vendor Advisory bugzilla.redhat.com text/html	CONFIRM bugzilla.redhat.com/show_bug.cgi?id=CVE-2017-12196
Red Hat Customer Portal	Vendor Advisory access.redhat.com text/html	REDHAT RHSA-2018:0478

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 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	6.0.0	All	All	All
Application	Redhat	Jboss Fuse	6.0.0	All	All	All
Application	Redhat	Undertow	1.4.24	All	All	All
Application	Redhat	Undertow	2.0.2	All	All	All
Application	Redhat	Undertow	1.4.24	All	All	All
Application	Redhat	Undertow	2.0.2	All	All	All
Application	Redhat	Undertow	All	All	All	All
Application	Redhat	Virtualization	4.0	All	All	All

Application	Redhat	Virtualization	4.0	All	All	All

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:6.0.0:*:*:*:*:*:*:*

cpe:2.3:a:redhat:jboss_fuse:6.0.0:*:*:*:*:*:*:*

cpe:2.3:a:redhat:undertow:1.4.24:*:*:*:*:*:*:*

cpe:2.3:a:redhat:undertow:2.0.2:*:*:*:*:*:*:*

cpe:2.3:a:redhat:undertow:1.4.24:*:*:*:*:*:*:*

cpe:2.3:a:redhat:undertow:2.0.2:*:*:*:*:*:*:*

cpe:2.3:a:redhat:undertow:*:*:*:*:*:*:*:*

cpe:2.3:a:redhat:virtualization:4.0:*:*:*:*:*:*:*

cpe:2.3:a:redhat:virtualization:4.0:*:*:*:*:*:*:*

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→