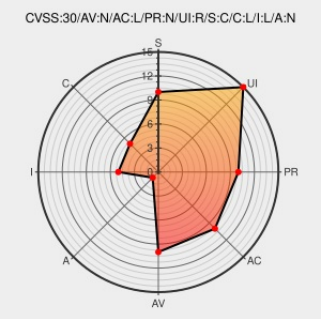
CVE-2017-7559

Published on: 01/10/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:41 PM UTC

CVE-2017-7559

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



Certain versions of Undertow from Redhat contain the following vulnerability:

In Undertow 2.x before 2.0.0.Alpha2, 1.4.x before 1.4.17.Final, and 1.3.x before 1.3.31.Final, it was found that the fix for CVE-2017-2666 was incomplete and invalid characters are still allowed in the query string and path parameters. This could be exploited, in conjunction with a proxy that also permitted the invalid characters but with a different interpretation, to inject data into the HTTP response. By manipulating the HTTP response the attacker could poison a web-cache, perform an XSS attack, or obtain sensitive information from requests other than their own.

CVE-2017-7559 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **Red Hat, Inc.** - **undertow** version **2.x before 2.0.0.Alpha2**

Affected Vendor/Software: **Red Hat, Inc.** - **undertow** version **1.4.x before 1.4.17.Final**

Affected Vendor/Software: **Red Hat, Inc.** - **undertow** version **1.3.x before 1.3.31.Final**

CVSS3 Score: 6.1 - MEDIUM

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	REQUIRED
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
CHANGED	LOW	LOW	NONE

CVSS2 Score: 5.8 - MEDIUM

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

Impact	Impact	Impact
PARTIAL	PARTIAL	NONE

CVE References

Description	Tags	Link
Red Hat Customer Portal	Vendor Advisory access.redhat.com text/html	REDHAT RHSA-2017:3455
Red Hat Customer Portal	Vendor Advisory access.redhat.com text/html	REDHAT RHSA-2018:1322
Red Hat Customer Portal	Vendor Advisory access.redhat.com text/html	REDHAT RHSA-2018:0004
1481665 – (CVE-2017-7559) CVE-2017-7559 undertow: HTTP Request smuggling vulnerability (incomplete fix of CVE-2017-2666)	Issue Tracking Vendor Advisory bugzilla.redhat.com text/html	CONFIRM bugzilla.redhat.com/show_bug.cgi?id=CVE-2017-7559
Red Hat Customer Portal	Vendor Advisory access.redhat.com text/html	REDHAT RHSA-2017:3454
Red Hat Customer Portal	Vendor Advisory access.redhat.com text/html	REDHAT RHSA-2018:0005
[UNDERTOW-1251] CVE-2017-2666 wildfly-undertow: undertow: HTTP Request smuggling vulnerability due to permitting invalid characters in HTTP requests [eap-7.0.5] - Red Hat Issue Tracker	Issue Tracking Vendor Advisory issues.jboss.org text/html	CONFIRM issues.jboss.org/browse/UNDERTOW-1251
Red Hat Customer Portal	Vendor Advisory access.redhat.com text/html	REDHAT RHSA-2017:3456
Red Hat Customer Portal	Vendor Advisory access.redhat.com text/html	REDHAT RHSA-2017:3458
Red Hat Customer Portal	Vendor Advisory access.redhat.com text/html	REDHAT RHSA-2018:0003
Red Hat Customer Portal	Vendor Advisory access.redhat.com text/html	REDHAT RHSA-2018:0002

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language

Type	Vendor	Product	Version	Update	Edition	Language
Application	Redhat	Undertow	All	All	All	All
Application	Redhat	Undertow	2.0.0	alpha1	All	All
Application	Redhat	Undertow	All	All	All	All
Application	Redhat	Undertow	2.0.0	alpha1	All	All

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

cpe:2.3:a:redhat:undertow:2.0.0:alpha1:*:*:*:*:*:*:

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

cpe:2.3:a:redhat:undertow:2.0.0:alpha1:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→