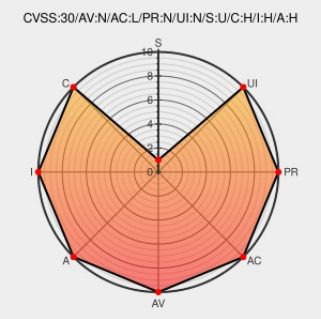
CVE-2015-8863

Published on: 05/06/2016 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:13 PM UTC

CVE-2015-8863

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



Certain versions of Jq from Jq Project contain the following vulnerability:

Off-by-one error in the tokenadd function in jv_parse.c in jq allows remote attackers to cause a denial of service (crash) via a long JSON-encoded number, which triggers a heap-based buffer overflow.

CVE-2015-8863 has been assigned by security@debian.org to track the vulnerability - currently rated as CRITICAL severity.

CVSS3 Score: 9.8 - CRITICAL

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

CVSS2 Score: 10 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
oss-security - Re: CVE Request: jq: heap buffer overflow in tokenadd() function	www.openwall.com text/html	MLIST [oss-security] 20160423 Re: CVE Request: jq: heap buffer overflow in tokenadd() function

Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2016:1099
Heap buffer overflow in tokenadd() (fix #105) · stedolan/jq@8eb1367 · GitHub	Patch github.com text/html	CONFIRM github.com/stedolan/jq/commit/8eb1367ca44e772963e704a700ef72ae2e12babd
Heap-based buffer overflow in check_literal() · Issue #995 · stedolan/jq · GitHub	github.com text/html	CONFIRM github.com/stedolan/jq/issues/995
openSUSE-SU-2016:1212-1: moderate: Security update for jq	lists.opensuse.org text/html	SUSE openSUSE-SU-2016:1212
jq: Buffer overflow (GLSA 201612-20) — Gentoo security	security.gentoo.org text/html	GENTOO GLSA-201612-20
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2016:1106
openSUSE-SU-2016:1214-1: moderate: Security update for jq	lists.opensuse.org text/html	SUSE openSUSE-SU-2016:1214
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2016:1098
#802231 - jq: CVE-2015-8863: Heap buffer overflow in tokenadd() - Debian Bug report logs	bugs.debian.org text/html	CONFIRM bugs.debian.org/cgi-bin/bugreport.cgi?bug=802231
oss-security - CVE Request: jq: heap buffer overflow in tokenadd() function	www.openwall.com text/html	MLIST [oss-security] 20160423 CVE Request: jq: heap buffer overflow in tokenadd() function

Related QID Numbers

900007 CBL-Mariner Linux Security Update for jq 1.5

901427 Common Base Linux Mariner (CBL-Mariner) Security Update for jq (6504-1)

902929 Common Base Linux Mariner (CBL-Mariner) Security Update for jq (1972)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Jq Project	Jq	All	All	All	All
Operating System	Opensuse	Leap	42.1	All	All	All

Operating System	Opensuse	Leap	42.1	All	All	All
Operating System	Opensuse	Opensuse	13.2	All	All	All
Operating System	Opensuse	Opensuse	13.2	All	All	All

cpe:2.3:a:jq_project:jq:*:*:*:*:*:*:*:*:

cpe:2.3:o:opensuse:leap:42.1:*:*:*:*:*:*:*:

cpe:2.3:o:opensuse:leap:42.1:*:*:*:*:*:*:*:

cpe:2.3:o:opensuse:opensuse:13.2:*:*:*:*:*:*:*:

cpe:2.3:o:opensuse:opensuse:13.2:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→