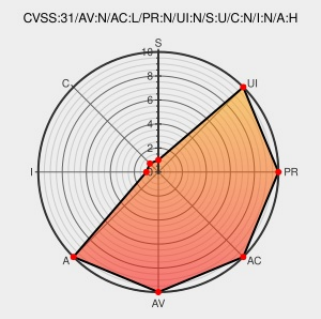
CVE-2015-2929

Published on: 01/24/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:20 PM UTC

CVE-2015-2929

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



Certain versions of Tor from Torproject contain the following vulnerability:

The Hidden Service (HS) client implementation in Tor before 0.2.4.27, 0.2.5.x before 0.2.5.12, and 0.2.6.x before 0.2.6.7 allows remote servers to cause a denial of service (assertion failure and application exit) via a malformed HS descriptor.

CVE-2015-2929 has been assigned by security@debian.org to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **The Tor Project** - **Tor** version **before 0.2.4.27**

Affected Vendor/Software: **The Tor Project** - **Tor** version **0.2.5.x before 0.2.5.12**

Affected Vendor/Software: **The Tor Project** - **Tor** version **0.2.6.x before 0.2.6.7**

CVSS3 Score: 7.5 - HIGH

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

CVSS2 Score: 5 - MEDIUM

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

CVE References

Description	Tags	Link
#15601 (Remote assert in hidden service client code) – Tor Bug Tracker & Wiki	Vendor Advisory trac.torproject.org text/html	MISC trac.torproject.org/projects/tor/ticket/15601
oss-security - CVE Request: tor: new upstream releases (0.2.6.7, 0.2.5.12 and 0.2.4.27) fixing security issues	Mailing List Third Party Advisory openwall.com text/html	MISC openwall.com/lists/oss-security/2015/04/06/5

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Torproject	Tor	All	All	All	All
Application	Torproject	Tor	All	All	All	All

cpe:2.3:a:torproject:tor:*:*:*:*:*:*:*:*:

cpe:2.3:a:torproject:tor:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→