



CVE-2013-7295

Published on: 01/17/2014 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:34 PM UTC

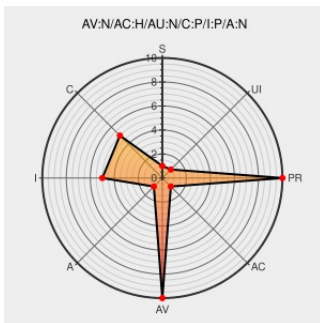
CVE-2013-7295

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



Certain versions of [Tor](#) from [Torproject](#) contain the following vulnerability:

Tor before 0.2.4.20, when OpenSSL 1.x is used in conjunction with a certain HardwareAccel setting on Intel Sandy Bridge and Ivy Bridge platforms, does not properly generate random numbers for (1) relay identity keys and (2) hidden-service identity keys, which might make it easier for remote attackers to bypass cryptographic protection

mechanisms via unspecified vectors.

CVE-2013-7295 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **4 - MEDIUM**

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

CVE References

Description	Tags	Link
[tor-talk] Tor 0.2.4.20 is released	Vendor Advisory lists.torproject.org text/html	MLIST [tor-talk] 20131223 Tor 0.2.4.20 is released
openSUSE-SU-2014:0143-1: moderate: update for tor	lists.opensuse.org text/html	SUSE openSUSE-SU-2014:0143

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	Torproject	Tor	0.2.4.1	alpha	All	All
Application	Torproject	Tor	0.2.4.10	alpha	All	All
Application	Torproject	Tor	0.2.4.11	alpha	All	All
Application	Torproject	Tor	0.2.4.12	alpha	All	All
Application	Torproject	Tor	0.2.4.13	alpha	All	All
Application	Torproject	Tor	0.2.4.14	alpha	All	All
Application	Torproject	Tor	0.2.4.15	rc	All	All
Application	Torproject	Tor	0.2.4.16	rc	All	All
Application	Torproject	Tor	0.2.4.17	rc	All	All
Application	Torproject	Tor	0.2.4.18	rc	All	All
Application	Torproject	Tor	0.2.4.2	alpha	All	All
Application	Torproject	Tor	0.2.4.3	alpha	All	All
Application	Torproject	Tor	0.2.4.4	alpha	All	All
Application	Torproject	Tor	0.2.4.5	alpha	All	All
Application	Torproject	Tor	0.2.4.6	alpha	All	All
Application	Torproject	Tor	0.2.4.7	alpha	All	All
Application	Torproject	Tor	0.2.4.8	alpha	All	All
Application	Torproject	Tor	0.2.4.9	alpha	All	All
Application	Torproject	Tor	All	All	All	All
Application	Torproject	Tor	0.2.4.1	alpha	All	All
Application	Torproject	Tor	0.2.4.10	alpha	All	All
Application	Torproject	Tor	0.2.4.11	alpha	All	All
Application	Torproject	Tor	0.2.4.12	alpha	All	All
Application	Torproject	Tor	0.2.4.13	alpha	All	All
Application	Torproject	Tor	0.2.4.14	alpha	All	All
Application	Torproject	Tor	0.2.4.15	rc	All	All
Application	Torproject	Tor	0.2.4.16	rc	All	All
Application	Torproject	Tor	0.2.4.17	rc	All	All
Application	Torproject	Tor	0.2.4.18	rc	All	All
Application	Torproject	Tor	0.2.4.2	alpha	All	All
Application	Torproject	Tor	0.2.4.3	alpha	All	All

Application	Torproject	Tor	0.2.4.4	alpha	All	All
Application	Torproject	Tor	0.2.4.5	alpha	All	All
Application	Torproject	Tor	0.2.4.6	alpha	All	All
Application	Torproject	Tor	0.2.4.7	alpha	All	All
Application	Torproject	Tor	0.2.4.8	alpha	All	All
Application	Torproject	Tor	0.2.4.9	alpha	All	All
cpe:2.3:a:torproject:tor:0.2.4.1:alpha:*****:.*:						
cpe:2.3:a:torproject:tor:0.2.4.10:alpha:*****:.*:						
cpe:2.3:a:torproject:tor:0.2.4.11:alpha:*****:.*:						
cpe:2.3:a:torproject:tor:0.2.4.12:alpha:*****:.*:						
cpe:2.3:a:torproject:tor:0.2.4.13:alpha:*****:.*:						
cpe:2.3:a:torproject:tor:0.2.4.14:alpha:*****:.*:						
cpe:2.3:a:torproject:tor:0.2.4.15:rc:*****:.*:						
cpe:2.3:a:torproject:tor:0.2.4.16:rc:*****:.*:						
cpe:2.3:a:torproject:tor:0.2.4.17:rc:*****:.*:						
cpe:2.3:a:torproject:tor:0.2.4.18:rc:*****:.*:						
cpe:2.3:a:torproject:tor:0.2.4.2:alpha:*****:.*:						
cpe:2.3:a:torproject:tor:0.2.4.3:alpha:*****:.*:						
cpe:2.3:a:torproject:tor:0.2.4.4:alpha:*****:.*:						
cpe:2.3:a:torproject:tor:0.2.4.5:alpha:*****:.*:						
cpe:2.3:a:torproject:tor:0.2.4.6:alpha:*****:.*:						
cpe:2.3:a:torproject:tor:0.2.4.7:alpha:*****:.*:						
cpe:2.3:a:torproject:tor:0.2.4.8:alpha:*****:.*:						
cpe:2.3:a:torproject:tor:0.2.4.9:alpha:*****:.*:						
cpe:2.3:a:torproject:tor:*****:.*:						
cpe:2.3:a:torproject:tor:0.2.4.1:alpha:*****:.*:						
cpe:2.3:a:torproject:tor:0.2.4.10:alpha:*****:.*:						
cpe:2.3:a:torproject:tor:0.2.4.11:alpha:*****:.*:						
cpe:2.3:a:torproject:tor:0.2.4.12:alpha:*****:.*:						
cpe:2.3:a:torproject:tor:0.2.4.13:alpha:*****:.*:						

cpe:2.3:a:torproject:tor:0.2.4.14:alpha:~::~~::~~::~~::~~::~~:::
cpe:2.3:a:torproject:tor:0.2.4.15:rc:~::~~::~~::~~::~~::~~:::
cpe:2.3:a:torproject:tor:0.2.4.16:rc:~::~~::~~::~~::~~::~~:::
cpe:2.3:a:torproject:tor:0.2.4.17:rc:~::~~::~~::~~::~~::~~:::
cpe:2.3:a:torproject:tor:0.2.4.18:rc:~::~~::~~::~~::~~::~~:::
cpe:2.3:a:torproject:tor:0.2.4.2:alpha:~::~~::~~::~~::~~::~~:::
cpe:2.3:a:torproject:tor:0.2.4.3:alpha:~::~~::~~::~~::~~::~~:::
cpe:2.3:a:torproject:tor:0.2.4.4:alpha:~::~~::~~::~~::~~::~~:::
cpe:2.3:a:torproject:tor:0.2.4.5:alpha:~::~~::~~::~~::~~::~~:::
cpe:2.3:a:torproject:tor:0.2.4.6:alpha:~::~~::~~::~~::~~::~~:::
cpe:2.3:a:torproject:tor:0.2.4.7:alpha:~::~~::~~::~~::~~::~~:::
cpe:2.3:a:torproject:tor:0.2.4.8:alpha:~::~~::~~::~~::~~::~~:::
cpe:2.3:a:torproject:tor:0.2.4.9:alpha:~::~~::~~::~~::~~::~~:::

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID→](#)