



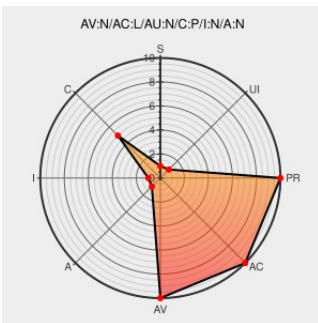
Last Modified on: 03/23/2021 11:24:58 PM UTC

CVE-2006-3419

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF 

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

Tor before 0.1.1.20 uses OpenSSL pseudo-random bytes (RAND_pseudo_bytes) instead of cryptographically strong RAND_bytes, and seeds the entropy value at start-up with 160-bit chunks without reseeding, which makes it easier for attackers to conduct brute force guessing attacks.

CVE-2006-3419 has been assigned by  cve@mitre.org to track the vulnerability

CVSS2 Score: 5 - MEDIUM

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

CVE References

Description	Tags	Link
404 Not Found	tor.eff.org text/plain Inactive Link Not Archived	 CONFIRM tor.eff.org/cvs/tor/ChangeLog
Gentoo Linux Documentation -- Tor: Several vulnerabilities	security.gentoo.org text/html	 GENTOO GLSA-200606-04
No Description Provided	www.osvdb.org Inactive Link Not Archived	 OSVDB 25880
Gentoo update for tor - Advisories - Secunia	Patch Vendor Advisory web.archive.org text/html	 SECUNIA 20514

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that

By selecting these links, you may be leaving CVEreport's website. We have provided these links to other resources 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	Tor	Tor	0.0.2	All	All	All
Application	Tor	Tor	0.0.2_pre13	All	All	All
Application	Tor	Tor	0.0.2_pre14	All	All	All
Application	Tor	Tor	0.0.2_pre15	All	All	All
Application	Tor	Tor	0.0.2_pre16	All	All	All
Application	Tor	Tor	0.0.2_pre17	All	All	All
Application	Tor	Tor	0.0.2_pre18	All	All	All
Application	Tor	Tor	0.0.2_pre19	All	All	All
Application	Tor	Tor	0.0.2_pre20	All	All	All
Application	Tor	Tor	0.0.2_pre21	All	All	All
Application	Tor	Tor	0.0.2_pre22	All	All	All
Application	Tor	Tor	0.0.2_pre23	All	All	All
Application	Tor	Tor	0.0.2_pre24	All	All	All
Application	Tor	Tor	0.0.2_pre25	All	All	All
Application	Tor	Tor	0.0.2_pre26	All	All	All
Application	Tor	Tor	0.0.2_pre27	All	All	All
Application	Tor	Tor	0.0.3	All	All	All
Application	Tor	Tor	0.0.4	All	All	All
Application	Tor	Tor	0.0.5	All	All	All
Application	Tor	Tor	0.0.6	All	All	All
Application	Tor	Tor	0.0.6.1	All	All	All
Application	Tor	Tor	0.0.6.2	All	All	All
Application	Tor	Tor	0.0.7	All	All	All
Application	Tor	Tor	0.0.7.1	All	All	All
Application	Tor	Tor	0.0.7.2	All	All	All
Application	Tor	Tor	0.0.7.3	All	All	All
Application	Tor	Tor	0.0.8	All	All	All
Application	Tor	Tor	0.0.8.1	All	All	All

Application	Tor	Tor	0.0.9	All	All	All
Application	Tor	Tor	0.0.9.1	All	All	All
Application	Tor	Tor	0.0.9.10	All	All	All
Application	Tor	Tor	0.0.9.2	All	All	All
Application	Tor	Tor	0.0.9.3	All	All	All
Application	Tor	Tor	0.0.9.4	All	All	All
Application	Tor	Tor	0.0.9.5	All	All	All
Application	Tor	Tor	0.0.9.6	All	All	All
Application	Tor	Tor	0.0.9.7	All	All	All
Application	Tor	Tor	0.0.9.8	All	All	All
Application	Tor	Tor	0.0.9.9	All	All	All
Application	Tor	Tor	0.1.0.1	All	All	All
Application	Tor	Tor	0.1.0.10	All	All	All
Application	Tor	Tor	0.1.0.11	All	All	All
Application	Tor	Tor	0.1.0.12	All	All	All
Application	Tor	Tor	0.1.0.13	All	All	All
Application	Tor	Tor	0.1.0.14	All	All	All
Application	Tor	Tor	0.1.0.15	All	All	All
Application	Tor	Tor	0.1.0.16	All	All	All
Application	Tor	Tor	0.1.0.17	All	All	All
Application	Tor	Tor	0.1.0.18	All	All	All
Application	Tor	Tor	0.1.0.19	All	All	All
Application	Tor	Tor	0.1.0.2	All	All	All
Application	Tor	Tor	0.1.0.3	All	All	All
Application	Tor	Tor	0.1.0.4	All	All	All
Application	Tor	Tor	0.1.0.5	All	All	All
Application	Tor	Tor	0.1.0.6	All	All	All
Application	Tor	Tor	0.1.0.7	All	All	All
Application	Tor	Tor	0.1.0.8	All	All	All
Application	Tor	Tor	0.1.0.9	All	All	All
Application	Tor	Tor	0.1.1.10_alpha	All	All	All
Application	Tor	Tor	0.1.1.1_alpha	All	All	All
Application	Tor	Tor	0.1.1.2_alpha	All	All	All
Application	Tor	Tor	0.1.1.3_alpha	All	All	All
Application	Tor	Tor	0.1.1.4_alpha	All	All	All
Application	Tor	Tor	0.1.1.5_alpha	All	All	All

Application	Tor	Tor	0.1.1.6_alpha	All	All	All
Application	Tor	Tor	0.1.1.6_alpha	All	All	All
Application	Tor	Tor	0.1.1.7_alpha	All	All	All
Application	Tor	Tor	0.1.1.8_alpha	All	All	All
Application	Tor	Tor	0.1.1.9_alpha	All	All	All
Application	Tor	Tor	0.0.2	All	All	All
Application	Tor	Tor	0.0.2_pre13	All	All	All
Application	Tor	Tor	0.0.2_pre14	All	All	All
Application	Tor	Tor	0.0.2_pre15	All	All	All
Application	Tor	Tor	0.0.2_pre16	All	All	All
Application	Tor	Tor	0.0.2_pre17	All	All	All
Application	Tor	Tor	0.0.2_pre18	All	All	All
Application	Tor	Tor	0.0.2_pre19	All	All	All
Application	Tor	Tor	0.0.2_pre20	All	All	All
Application	Tor	Tor	0.0.2_pre21	All	All	All
Application	Tor	Tor	0.0.2_pre22	All	All	All
Application	Tor	Tor	0.0.2_pre23	All	All	All
Application	Tor	Tor	0.0.2_pre24	All	All	All
Application	Tor	Tor	0.0.2_pre25	All	All	All
Application	Tor	Tor	0.0.2_pre26	All	All	All
Application	Tor	Tor	0.0.2_pre27	All	All	All
Application	Tor	Tor	0.0.3	All	All	All
Application	Tor	Tor	0.0.4	All	All	All
Application	Tor	Tor	0.0.5	All	All	All
Application	Tor	Tor	0.0.6	All	All	All
Application	Tor	Tor	0.0.6.1	All	All	All
Application	Tor	Tor	0.0.6.2	All	All	All
Application	Tor	Tor	0.0.7	All	All	All
Application	Tor	Tor	0.0.7.1	All	All	All
Application	Tor	Tor	0.0.7.2	All	All	All
Application	Tor	Tor	0.0.7.3	All	All	All
Application	Tor	Tor	0.0.8	All	All	All
Application	Tor	Tor	0.0.8.1	All	All	All
Application	Tor	Tor	0.0.9	All	All	All
Application	Tor	Tor	0.0.9.1	All	All	All
Application	Tor	Tor	0.0.9.10	All	All	All

Application	Tor	Tor	0.0.9.2	All	All	All
Application	Tor	Tor	0.0.9.3	All	All	All
Application	Tor	Tor	0.0.9.4	All	All	All
Application	Tor	Tor	0.0.9.5	All	All	All
Application	Tor	Tor	0.0.9.6	All	All	All
Application	Tor	Tor	0.0.9.7	All	All	All
Application	Tor	Tor	0.0.9.8	All	All	All
Application	Tor	Tor	0.0.9.9	All	All	All
Application	Tor	Tor	0.1.0.1	All	All	All
Application	Tor	Tor	0.1.0.10	All	All	All
Application	Tor	Tor	0.1.0.11	All	All	All
Application	Tor	Tor	0.1.0.12	All	All	All
Application	Tor	Tor	0.1.0.13	All	All	All
Application	Tor	Tor	0.1.0.14	All	All	All
Application	Tor	Tor	0.1.0.15	All	All	All
Application	Tor	Tor	0.1.0.16	All	All	All
Application	Tor	Tor	0.1.0.17	All	All	All
Application	Tor	Tor	0.1.0.18	All	All	All
Application	Tor	Tor	0.1.0.19	All	All	All
Application	Tor	Tor	0.1.0.2	All	All	All
Application	Tor	Tor	0.1.0.3	All	All	All
Application	Tor	Tor	0.1.0.4	All	All	All
Application	Tor	Tor	0.1.0.5	All	All	All
Application	Tor	Tor	0.1.0.6	All	All	All
Application	Tor	Tor	0.1.0.7	All	All	All
Application	Tor	Tor	0.1.0.8	All	All	All
Application	Tor	Tor	0.1.0.9	All	All	All
Application	Tor	Tor	0.1.1.10_alpha	All	All	All
Application	Tor	Tor	0.1.1.1_alpha	All	All	All
Application	Tor	Tor	0.1.1.2_alpha	All	All	All
Application	Tor	Tor	0.1.1.3_alpha	All	All	All
Application	Tor	Tor	0.1.1.4_alpha	All	All	All
Application	Tor	Tor	0.1.1.5_alpha	All	All	All
Application	Tor	Tor	0.1.1.6_alpha	All	All	All
Application	Tor	Tor	0.1.1.7_alpha	All	All	All

Application	Tor	Tor	0.1.1.8_alpha	All	All	All
Application	Tor	Tor	0.1.1.9_alpha	All	All	All
cpe:2.3:a:tor:tor:0.0.2:*****:*						
cpe:2.3:a:tor:tor:0.0.2_pre13:*****:*						
cpe:2.3:a:tor:tor:0.0.2_pre14:*****:*						
cpe:2.3:a:tor:tor:0.0.2_pre15:*****:*						
cpe:2.3:a:tor:tor:0.0.2_pre16:*****:*						
cpe:2.3:a:tor:tor:0.0.2_pre17:*****:*						
cpe:2.3:a:tor:tor:0.0.2_pre18:*****:*						
cpe:2.3:a:tor:tor:0.0.2_pre19:*****:*						
cpe:2.3:a:tor:tor:0.0.2_pre20:*****:*						
cpe:2.3:a:tor:tor:0.0.2_pre21:*****:*						
cpe:2.3:a:tor:tor:0.0.2_pre22:*****:*						
cpe:2.3:a:tor:tor:0.0.2_pre23:*****:*						
cpe:2.3:a:tor:tor:0.0.2_pre24:*****:*						
cpe:2.3:a:tor:tor:0.0.2_pre25:*****:*						
cpe:2.3:a:tor:tor:0.0.2_pre26:*****:*						
cpe:2.3:a:tor:tor:0.0.2_pre27:*****:*						
cpe:2.3:a:tor:tor:0.0.3:*****:*						
cpe:2.3:a:tor:tor:0.0.4:*****:*						
cpe:2.3:a:tor:tor:0.0.5:*****:*						
cpe:2.3:a:tor:tor:0.0.6:*****:*						
cpe:2.3:a:tor:tor:0.0.6.1:*****:*						
cpe:2.3:a:tor:tor:0.0.6.2:*****:*						
cpe:2.3:a:tor:tor:0.0.7:*****:*						
cpe:2.3:a:tor:tor:0.0.7.1:*****:*						
cpe:2.3:a:tor:tor:0.0.7.2:*****:*						
cpe:2.3:a:tor:tor:0.0.7.3:*****:*						
cpe:2.3:a:tor:tor:0.0.8:*****:*						

cpe:2.3:a:tor:tor:0.0.8.1:*****:
cpe:2.3:a:tor:tor:0.0.9:*****:
cpe:2.3:a:tor:tor:0.0.9.1:*****:
cpe:2.3:a:tor:tor:0.0.9.10:*****:
cpe:2.3:a:tor:tor:0.0.9.2:*****:
cpe:2.3:a:tor:tor:0.0.9.3:*****:
cpe:2.3:a:tor:tor:0.0.9.4:*****:
cpe:2.3:a:tor:tor:0.0.9.5:*****:
cpe:2.3:a:tor:tor:0.0.9.6:*****:
cpe:2.3:a:tor:tor:0.0.9.7:*****:
cpe:2.3:a:tor:tor:0.0.9.8:*****:
cpe:2.3:a:tor:tor:0.0.9.9:*****:
cpe:2.3:a:tor:tor:0.1.0.1:*****:
cpe:2.3:a:tor:tor:0.1.0.10:*****:
cpe:2.3:a:tor:tor:0.1.0.11:*****:
cpe:2.3:a:tor:tor:0.1.0.12:*****:
cpe:2.3:a:tor:tor:0.1.0.13:*****:
cpe:2.3:a:tor:tor:0.1.0.14:*****:
cpe:2.3:a:tor:tor:0.1.0.15:*****:
cpe:2.3:a:tor:tor:0.1.0.16:*****:
cpe:2.3:a:tor:tor:0.1.0.17:*****:
cpe:2.3:a:tor:tor:0.1.0.18:*****:
cpe:2.3:a:tor:tor:0.1.0.19:*****:
cpe:2.3:a:tor:tor:0.1.0.2:*****:
cpe:2.3:a:tor:tor:0.1.0.3:*****:
cpe:2.3:a:tor:tor:0.1.0.4:*****:
cpe:2.3:a:tor:tor:0.1.0.5:*****:
cpe:2.3:a:tor:tor:0.1.0.6:*****:
cpe:2.3:a:tor:tor:0.1.0.7:*****:

cpe:2.3:a:tor:tor:0.1.0./:~::~::~:
cpe:2.3:a:tor:tor:0.1.0.8::~::~:
cpe:2.3:a:tor:tor:0.1.0.9::~::~:
cpe:2.3:a:tor:tor:0.1.1.10_alpha::~::~:
cpe:2.3:a:tor:tor:0.1.1.1_alpha::~::~:
cpe:2.3:a:tor:tor:0.1.1.2_alpha::~::~:
cpe:2.3:a:tor:tor:0.1.1.3_alpha::~::~:
cpe:2.3:a:tor:tor:0.1.1.4_alpha::~::~:
cpe:2.3:a:tor:tor:0.1.1.5_alpha::~::~:
cpe:2.3:a:tor:tor:0.1.1.6_alpha::~::~:
cpe:2.3:a:tor:tor:0.1.1.7_alpha::~::~:
cpe:2.3:a:tor:tor:0.1.1.8_alpha::~::~:
cpe:2.3:a:tor:tor:0.1.1.9_alpha::~::~:
cpe:2.3:a:tor:tor:0.0.2::~::~:
cpe:2.3:a:tor:tor:0.0.2_pre13::~::~:
cpe:2.3:a:tor:tor:0.0.2_pre14::~::~:
cpe:2.3:a:tor:tor:0.0.2_pre15::~::~:
cpe:2.3:a:tor:tor:0.0.2_pre16::~::~:
cpe:2.3:a:tor:tor:0.0.2_pre17::~::~:
cpe:2.3:a:tor:tor:0.0.2_pre18::~::~:
cpe:2.3:a:tor:tor:0.0.2_pre19::~::~:
cpe:2.3:a:tor:tor:0.0.2_pre20::~::~:
cpe:2.3:a:tor:tor:0.0.2_pre21::~::~:
cpe:2.3:a:tor:tor:0.0.2_pre22::~::~:
cpe:2.3:a:tor:tor:0.0.2_pre23::~::~:
cpe:2.3:a:tor:tor:0.0.2_pre24::~::~:
cpe:2.3:a:tor:tor:0.0.2_pre25::~::~:
cpe:2.3:a:tor:tor:0.0.2_pre26::~::~:
cpe:2.3:a:tor:tor:0.0.2_pre27::~::~:

cpe:2.3:a:tor:tor:0.0.3:*****:
cpe:2.3:a:tor:tor:0.0.4:*****:
cpe:2.3:a:tor:tor:0.0.5:*****:
cpe:2.3:a:tor:tor:0.0.6:*****:
cpe:2.3:a:tor:tor:0.0.6.1:*****:
cpe:2.3:a:tor:tor:0.0.6.2:*****:
cpe:2.3:a:tor:tor:0.0.7:*****:
cpe:2.3:a:tor:tor:0.0.7.1:*****:
cpe:2.3:a:tor:tor:0.0.7.2:*****:
cpe:2.3:a:tor:tor:0.0.7.3:*****:
cpe:2.3:a:tor:tor:0.0.8:*****:
cpe:2.3:a:tor:tor:0.0.8.1:*****:
cpe:2.3:a:tor:tor:0.0.9:*****:
cpe:2.3:a:tor:tor:0.0.9.1:*****:
cpe:2.3:a:tor:tor:0.0.9.10:*****:
cpe:2.3:a:tor:tor:0.0.9.2:*****:
cpe:2.3:a:tor:tor:0.0.9.3:*****:
cpe:2.3:a:tor:tor:0.0.9.4:*****:
cpe:2.3:a:tor:tor:0.0.9.5:*****:
cpe:2.3:a:tor:tor:0.0.9.6:*****:
cpe:2.3:a:tor:tor:0.0.9.7:*****:
cpe:2.3:a:tor:tor:0.0.9.8:*****:
cpe:2.3:a:tor:tor:0.0.9.9:*****:
cpe:2.3:a:tor:tor:0.1.0.1:*****:
cpe:2.3:a:tor:tor:0.1.0.10:*****:
cpe:2.3:a:tor:tor:0.1.0.11:*****:
cpe:2.3:a:tor:tor:0.1.0.12:*****:
cpe:2.3:a:tor:tor:0.1.0.13:*****:

cpe:2.3:a:tor:tor:0.1.0.14:*****:
cpe:2.3:a:tor:tor:0.1.0.15:*****:
cpe:2.3:a:tor:tor:0.1.0.16:*****:
cpe:2.3:a:tor:tor:0.1.0.17:*****:
cpe:2.3:a:tor:tor:0.1.0.18:*****:
cpe:2.3:a:tor:tor:0.1.0.19:*****:
cpe:2.3:a:tor:tor:0.1.0.2:*****:
cpe:2.3:a:tor:tor:0.1.0.3:*****:
cpe:2.3:a:tor:tor:0.1.0.4:*****:
cpe:2.3:a:tor:tor:0.1.0.5:*****:
cpe:2.3:a:tor:tor:0.1.0.6:*****:
cpe:2.3:a:tor:tor:0.1.0.7:*****:
cpe:2.3:a:tor:tor:0.1.0.8:*****:
cpe:2.3:a:tor:tor:0.1.0.9:*****:
cpe:2.3:a:tor:tor:0.1.1.10_alpha:*****:
cpe:2.3:a:tor:tor:0.1.1.1_alpha:*****:
cpe:2.3:a:tor:tor:0.1.1.2_alpha:*****:
cpe:2.3:a:tor:tor:0.1.1.3_alpha:*****:
cpe:2.3:a:tor:tor:0.1.1.4_alpha:*****:
cpe:2.3:a:tor:tor:0.1.1.5_alpha:*****:
cpe:2.3:a:tor:tor:0.1.1.6_alpha:*****:
cpe:2.3:a:tor:tor:0.1.1.7_alpha:*****:
cpe:2.3:a:tor:tor:0.1.1.8_alpha:*****:
cpe:2.3:a:tor:tor:0.1.1.9_alpha:*****:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)