



CVE-2012-0051

Published on: 11/07/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:24 PM UTC

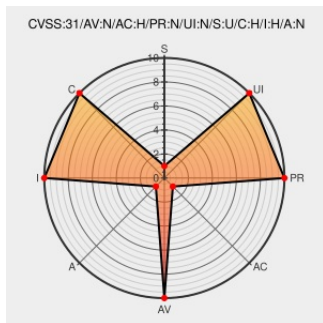
CVE-2012-0051

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



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

Tahoe-LAFS 1.9.0 fails to ensure integrity which allows remote attackers to corrupt mutable files or directories upon retrieval.

CVE-2012-0051 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: **tahoe-lafs** - **tahoe-lafs** version **1.10.0-2**

CVSS3 Score: **7.4 - HIGH**

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

CVSS2 Score: **5.8 - MEDIUM**

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

CVE References

Description	Tags	Link
oss-security - Re: Request for CVE for Vulnerability in Tahoe-LAFS 1.9.0	Mailing List Third Party Advisory www.openwall.com	MISC www.openwall.com/lists/oss-security/2012/01/26/9

	www.openwall.com text/html	
oss-security - Re: details about Tahoe-LAFS security problem #1654	Exploit Mailing List Third Party Advisory www.openwall.com text/html	 MISC www.openwall.com/lists/oss-security/2012/01/15/11
oss-security - Re: Request for CVE for Vulnerability in Tahoe-LAFS 1.9.0	Mailing List Third Party Advisory www.openwall.com text/html	 MISC www.openwall.com/lists/oss-security/2012/01/26/8
#1654 (integrity failure in mutable retrieve (SDMF+MDMF) in 1.9.0) – tahoe-lafs	Exploit Issue Tracking Vendor Advisory tahoe-lafs.org text/html	 CONFIRM tahoe-lafs.org/trac/tahoe-lafs/ticket/1654
oss-security - Re: Request for CVE for Vulnerability in Tahoe-LAFS 1.9.0	Mailing List Third Party Advisory www.openwall.com text/html	 MISC www.openwall.com/lists/oss-security/2012/01/26/7
CVE-2012-0051	Third Party Advisory security-tracker.debian.org text/html	 MISC security-tracker.debian.org/tracker/CVE-2012-0051

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
Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Application	Tahoe-lafs	Tahoe-lafs	1.9.0	All	All	All
Application	Tahoe-lafs	Tahoe-lafs	1.9.0	All	All	All

cpe:2.3:o:debian:debian_linux:10.0:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:8.0:*****:
cpe:2.3:o:debian:debian_linux:9.0:*****:
cpe:2.3:o:debian:debian_linux:10.0:*****:
cpe:2.3:o:debian:debian_linux:8.0:*****:
cpe:2.3:o:debian:debian_linux:9.0:*****:
cpe:2.3:a:tahoe-lafs:tahoe-lafs:1.9.0:*****:
cpe:2.3:a:tahoe-lafs:tahoe-lafs:1.9.0:*****:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID→](#)