

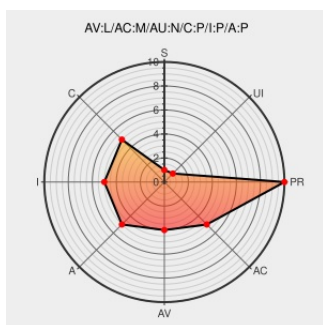


CVE-2011-2185

Published on: 07/26/2011 12:00:00 AM UTC

Last Modified on: 02/13/2023 12:08:08 AM UTC

CVE-2011-2185

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

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

Fabric before 1.1.0 allows local users to overwrite arbitrary files via a symlink attack on (1) a /tmp/fab.*.tar file or (2) certain other files in the top level of /tmp/.

CVE-2011-2185 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: **4.4 - MEDIUM**

Access
Vector

LOCAL

Access
Complexity

MEDIUM

Authentication

NONE

Confidentiality
Impact

PARTIAL

Integrity
Impact

PARTIAL

Availability
Impact

PARTIAL

CVE References

Description

Tags

Link

Bug 710462 – CVE-2011-2185 fabric: Use of insecure temporary file by uploading templates and projects to remote hosts

[bugzilla.redhat.com](#)
text/html

[CONFIRM bugzilla.redhat.com/show_bug.cgi?id=710462](https://bugzilla.redhat.com/show_bug.cgi?id=710462)

[SECURITY] Fedora 14 Update: fabric-0.9.7-1.fc14

[lists.fedoraproject.org](#)
text/html

[FEDORA FEDORA-2011-8964](#)

Patch
[code.fabfile.org](#)
application/gzip

[CONFIRM](#)
code.fabfile.org/projects/fabric/files/Fabric-1.1.0.tar.gz

#629003 - fabric is prone to file-overwrite security issue(s). - Debian Bug report logs

[bugs.debian.org](#)
text/html

[CONFIRM](#) bugs.debian.org/cgi-bin/bugreport.cgi?bug=629003

oss-security - Re: CVE Request -- fabric -- Use of insecure temporary file by uploading templates and projects to remote hosts

[www.openwall.com](#)
text/html

[MLIST \[oss-security\] 20110606 Re: CVE Request -- fabric -- Use of insecure temporary file by uploading templates and projects to remote hosts](#)

oss-security - CVE Request -- fabric -- Use of insecure temporary file by uploading templates and projects to remote hosts

www.openwall.com
[text/html](#)

 [MLIST \[oss-security\] 20110603 CVE Request -- fabric -- Use of insecure temporary file by uploading templates and projects to remote hosts](#)

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	Fabfile	Fabric	0.9	All	All	All
Application	Fabfile	Fabric	0.9.1	All	All	All
Application	Fabfile	Fabric	0.9.2	All	All	All
Application	Fabfile	Fabric	0.9.3	All	All	All
Application	Fabfile	Fabric	0.9.4	All	All	All
Application	Fabfile	Fabric	0.9.5	All	All	All
Application	Fabfile	Fabric	0.9.6	All	All	All
Application	Fabfile	Fabric	0.9.7	All	All	All
Application	Fabfile	Fabric	1.0.0	All	All	All
Application	Fabfile	Fabric	1.0.1	All	All	All
Application	Fabfile	Fabric	0.9	All	All	All
Application	Fabfile	Fabric	0.9.1	All	All	All
Application	Fabfile	Fabric	0.9.2	All	All	All
Application	Fabfile	Fabric	0.9.3	All	All	All
Application	Fabfile	Fabric	0.9.4	All	All	All
Application	Fabfile	Fabric	0.9.5	All	All	All
Application	Fabfile	Fabric	0.9.6	All	All	All
Application	Fabfile	Fabric	0.9.7	All	All	All
Application	Fabfile	Fabric	1.0.0	All	All	All
Application	Fabfile	Fabric	1.0.1	All	All	All
Application	Fabfile	Fabric	All	All	All	All

cpe:2.3:a:fabfile:fabric:0.9:*****:

cpe:2.3:a:fabfile:fabric:0.9.1:*****:

cpe:2.3:a:fabfile:fabric:0.9.2:*****:

cpe:2.3:a:fabfile:fabric:0.9.3:*****:
cpe:2.3:a:fabfile:fabric:0.9.4:*****:
cpe:2.3:a:fabfile:fabric:0.9.5:*****:
cpe:2.3:a:fabfile:fabric:0.9.6:*****:
cpe:2.3:a:fabfile:fabric:0.9.7:*****:
cpe:2.3:a:fabfile:fabric:1.0.0:*****:
cpe:2.3:a:fabfile:fabric:1.0.1:*****:
cpe:2.3:a:fabfile:fabric:0.9:*****:
cpe:2.3:a:fabfile:fabric:0.9.1:*****:
cpe:2.3:a:fabfile:fabric:0.9.2:*****:
cpe:2.3:a:fabfile:fabric:0.9.3:*****:
cpe:2.3:a:fabfile:fabric:0.9.4:*****:
cpe:2.3:a:fabfile:fabric:0.9.5:*****:
cpe:2.3:a:fabfile:fabric:0.9.6:*****:
cpe:2.3:a:fabfile:fabric:0.9.7:*****:
cpe:2.3:a:fabfile:fabric:1.0.0:*****:
cpe:2.3:a:fabfile:fabric:1.0.1:*****:
cpe:2.3:a:fabfile:fabric:*****:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

© [CVE.report](#) 2023   |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to 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](#)