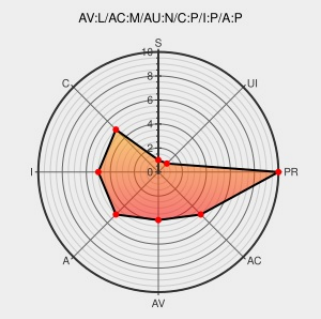
CVE-2011-2185

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	Access Complexity	Authentication
LOCAL	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	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
[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

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→