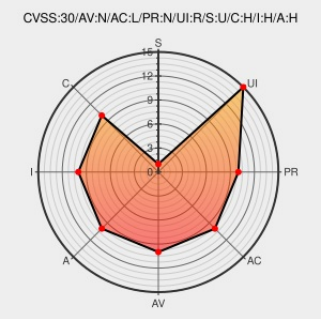
CVE-2017-17459

Published on: 12/07/2017 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:27 PM UTC

CVE-2017-17459

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Fossil from Fossil Scm contain the following vulnerability:

http_transport.c in Fossil before 2.4, when the SSH sync protocol is used, allows user-assisted remote attackers to execute arbitrary commands via an ssh URL with an initial dash character in the hostname, a related issue to CVE-2017-9800, CVE-2017-12836, CVE-2017-12976, CVE-2017-14176, CVE-2017-16228, CVE-2017-1000116, and CVE-2017-1000117.

CVE-2017-17459 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 8.8 - HIGH

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

CVSS2 Score: 9.3 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
Fossil: Check-in [1f63db59]	Patch, Vendor Advisory	CONFIRM www.fossil-scm.org/xfer/info/1f63db591c77108c

	www.fossil-scm.org text/html	
Fossil: Change Log	Release Notes Vendor Advisory www.fossil-scm.org text/html	CONFIRM www.fossil-scm.org/xfer/doc/trunk/www/changes.wiki#v2_4
Bug 1071709 – VUL-0: CVE-2017-17459: fossil: client-side code execution via specially crafted ssh:// URL (ProxyCommand)	Issue Tracking bugzilla.opensuse.org text/html	CONFIRM bugzilla.opensuse.org/show_bug.cgi?id=1071709
[SECURITY] Fedora 30 Update: fossil-2.8-1.fc30 - package-announce - Fedora Mailing-Lists	lists.fedoraproject.org text/html	FEDORA FEDORA-2019-f350634b40

Related QID Numbers

710268 Gentoo Linux Fossil User-assisted execution of arbitrary code Vulnerability (GLSA 201801-20)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Fossil Scm	Fossil	All	All	All	All
Application	Fossil Scm	Fossil	All	All	All	All

cpe:2.3:a:fossil_scm:fossil:*:*:*:*:*:*:*:*:

cpe:2.3:a:fossil_scm:fossil:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→