



CVE-2020-10174

Published on: 03/05/2020 12:00:00 AM UTC

Last Modified on: 01/01/2022 07:36:00 PM UTC

CVE-2020-10174

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

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

init_tmp in TeeJee.FileSystem.vala in Timeshift before 20.03 unsafely reuses a preexisting temporary directory in the predictable location /tmp/timeshift. It follows symlinks in this location or uses directories owned by unprivileged users. Because Timeshift also executes scripts under this location, an attacker can attempt to win a race condition to

replace scripts created by Timeshift with attacker-controlled scripts. Upon success, an attacker-controlled script is executed with full root privileges. This logic is practically always triggered when Timeshift runs regardless of the command-line arguments used.

CVE-2020-10174 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **7 - HIGH**

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

CVSS2 Score: **6.9 - MEDIUM**

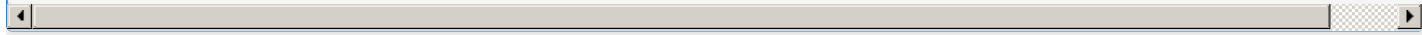
Access Vector	Access Complexity	Authentication
LOCAL	MEDIUM	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
-------------	------	------

Release v20.03 · teejee2008/timeshift · GitHub	Release Notes Third Party Advisory github.com text/html	 MISC github.com/teejee2008/timeshift/releases/tag/v20.03
USN-4312-1: Timeshift vulnerability Ubuntu security notices Ubuntu	usn.ubuntu.com text/html	 UBUNTU USN-4312-1
Bug 1165802 – VUL-0: CVE-2020-10174: timeshift: arbitrary local code execution due to unsafe usage of temporary directory in /tmp/timeshift	Issue Tracking Third Party Advisory bugzilla.suse.com text/html	 MISC bugzilla.suse.com/show_bug.cgi?id=1165802
Change TEMP_DIR permissions and path; Cleanup on exit; · teejee2008/timeshift@335b3d5 · GitHub	Patch Third Party Advisory github.com text/html	 MISC github.com/teejee2008/timeshift/commit/335b3d5398079278b8f7094c77bfd148b315
[SECURITY] Fedora 30 Update: timeshift-20.03-1.fc30 - package-announce - Fedora Mailing-Lists	lists.fedoraproject.org text/html	 FEDORA FEDORA-2020-1050d60507
[SECURITY] Fedora 31 Update: timeshift-20.03-1.fc31 - package-announce - Fedora Mailing-Lists	lists.fedoraproject.org text/html	 FEDORA FEDORA-2020-6b3ae09449
[SECURITY] Fedora 32 Update: timeshift-20.03-1.fc32 - package-announce - Fedora Mailing-Lists	lists.fedoraproject.org text/html	 FEDORA FEDORA-2020-c18248f61a
oss-security - CVE-2020-10174: timeshift: arbitrary local code execution due to unsafe usage of temporary directory in /tmp/timeshift	Third Party Advisory www.openwall.com text/html	 MLIST [oss-security] 20200306 CVE-2020-10174: timeshift: arbitrary local code execution due to unsafe usage of temporary directory in /tmp/timeshift

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	Canonical	Ubuntu Linux	19.10	All	All	All
Operating System	Fedoraproject	Fedora	30	All	All	All
Operating System	Fedoraproject	Fedora	31	All	All	All

Operating System	Fedoraproject	Fedora	32	All	All	All
Application	Timeshift Project	Timeshift	All	All	All	All
Application	Timeshift Project	Timeshift	All	All	All	All
cpe:2.3:o:canonical:ubuntu_linux:19.10:*****:						
cpe:2.3:o:fedoraproject:fedora:30:*****:						
cpe:2.3:o:fedoraproject:fedora:31:*****:						
cpe:2.3:o:fedoraproject:fedora:32:*****:						
cpe:2.3:a:timeshift_project:timeshift:*****:						
cpe:2.3:a:timeshift_project:timeshift:*****:						

No vendor comments have been submitted for this CVE

Social Mentions		
Source	Title	Posted (UTC)
← Previous ID Next ID→		