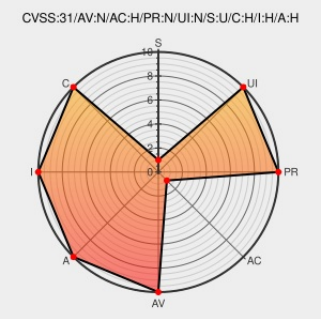
CVE-2020-7040

Published on: 01/21/2020 12:00:00 AM UTC

Last Modified on: 01/27/2023 03:17:00 PM UTC

CVE-2020-7040

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



Certain versions of Ubuntu Linux from Canonical contain the following vulnerability:

storeBackup.pl in storeBackup through 3.5 relies on the /tmp/storeBackup.lock pathname, which allows symlink attacks that possibly lead to privilege escalation. (Local users can also create a plain file named /tmp/storeBackup.lock to block use of storeBackup until an admin manually deletes that file.)

CVE-2020-7040 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 8.1 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	HIGH	NONE	NONE
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
oss-security - Re: CVE-2020-7040: storeBackup: denial of service and symlink attack vector via fixed lockfile path /tmp/storeBackup.lock	Mailing List Third Party Advisory www.openwall.com	MLIST [oss-security] 20200122 Re: CVE-2020-7040: storeBackup: denial of service and symlink attack vector via fixed lockfile path /tmp/storeBackup.lock

	text/html	
[SECURITY] [DLA 2095-1] storebackup security update	Mailing List Third Party Advisory lists.debian.org text/html	MLIST [debian-lts-announce] 20200205 [SECURITY] [DLA 2095-1] storebackup security update
oss-security - Re: CVE-2020-7040: storeBackup: denial of service and symlink attack vector via fixed lockfile path /tmp/storeBackup.lock	Mailing List Third Party Advisory www.openwall.com text/html	MLIST [oss-security] 20200121 Re: CVE-2020-7040: storeBackup: denial of service and symlink attack vector via fixed lockfile path /tmp/storeBackup.lock
oss-security - Re: CVE-2020-7040: storeBackup: denial of service and symlink attack vector via fixed lockfile path /tmp/storeBackup.lock	Mailing List Third Party Advisory www.openwall.com text/html	MLIST [oss-security] 20200123 Re: CVE-2020-7040: storeBackup: denial of service and symlink attack vector via fixed lockfile path /tmp/storeBackup.lock
oss-security - Re: CVE-2020-7040: storeBackup: denial of service and symlink attack vector via fixed lockfile path /tmp/storeBackup.lock	Mailing List Third Party Advisory www.openwall.com text/html	MLIST [oss-security] 20200122 Re: CVE-2020-7040: storeBackup: denial of service and symlink attack vector via fixed lockfile path /tmp/storeBackup.lock
oss-security - CVE-2020-7040: storeBackup: denial of service and symlink attack vector via fixed lockfile path /tmp/storeBackup.lock	Mailing List Third Party Advisory www.openwall.com text/html	MISC www.openwall.com/lists/oss-security/2020/01/20/3
[security-announce] openSUSE-SU-2020:0119-1: moderate: Security update f	Mailing List Patch Third Party Advisory lists.opensuse.org text/html	SUSE openSUSE-SU-2020:0119
Bug 1156767 – VUL-0: CVE-2020-7040: storeBackup: /tmp/storeBackup.lock default lock file location opens up a local DoS attack vector	Issue Tracking Third Party Advisory bugzilla.suse.com text/html	MISC bugzilla.suse.com/show_bug.cgi?id=CVE-2020-7040
oss-sec: CVE-2020-7040: storeBackup: denial of service and symlink attack vector via fixed lockfile path /tmp/storeBackup.lock	Mailing List Third Party Advisory seclists.org text/html	MLIST [oss-security] CVE-2020-7040: storeBackup: denial of service and symlink attack vector via fixed lockfile path /tmp/storeBackup.lock
USN-4508-1: StoreBackup vulnerability | Ubuntu security notices | Ubuntu	usn.ubuntu.com text/html	UBUNTU USN-4508-1

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	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Operating	Canonical	Ubuntu Linux	20.04	All	All	All

System						
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Application	Opensuse	Backports Sle	15.0	All	All	All
Application	Opensuse	Backports Sle	15.0	sp1	All	All
Application	Opensuse	Backports Sle	15.0	All	All	All
Application	Opensuse	Backports Sle	15.0	sp1	All	All
Operating System	Opensuse	Leap	15.1	All	All	All
Operating System	Opensuse	Leap	15.1	All	All	All
Application	Storebackup	Storebackup	All	All	All	All

cpe:2.3:o:canonical:ubuntu_linux:16.04:*:*:*:esm:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:18.04:*:*:*:lts:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:20.04:*:*:*:lts:*:*:*:

cpe:2.3:o:debian:debian_linux:8.0:*:*:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:8.0:*:*:*:*:*:*:*:

cpe:2.3:a:opensuse:backports_sle:15.0:*:*:*:*:*:*:*:

cpe:2.3:a:opensuse:backports_sle:15.0:sp1:*:*:*:*:*:*:

cpe:2.3:a:opensuse:backports_sle:15.0:*:*:*:*:*:*:*:

cpe:2.3:a:opensuse:backports_sle:15.0:sp1:*:*:*:*:*:*:

cpe:2.3:o:opensuse:leap:15.1:*:*:*:*:*:*:*:

cpe:2.3:o:opensuse:leap:15.1:*:*:*:*:*:*:*:

cpe:2.3:a:storebackup:storebackup:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report