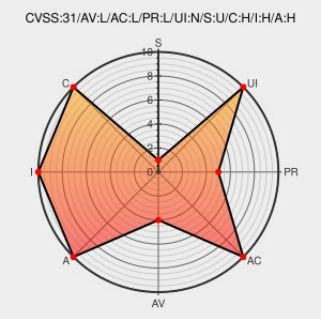
CVE-2017-18078

Published on: 01/29/2018 12:00:00 AM UTC

Last Modified on: 01/31/2022 06:24:00 PM UTC

CVE-2017-18078

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



Certain versions of Debian Linux from Debian contain the following vulnerability:

systemd-tmpfiles in systemd before 237 attempts to support ownership/permission changes on hardlinked files even if the fs.protected_hardlinks sysctl is turned off, which allows local users to bypass intended access restrictions via vectors involving a hard link to a file for which the user lacks write access, as demonstrated by changing the ownership of the /etc/passwd file.

CVE-2017-18078 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7.8 - HIGH

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

CVSS2 Score: 4.6 - MEDIUM

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
tmpfiles: unsafe handling of hard links and a race condition · Issue #7736 ·	Exploit Third Party Advisory	MISC github.com/systemd/systemd/issues/7736

systemd/systemd · GitHub	github.com text/html	
[SECURITY] [DLA 1762-1] systemd security update	Mailing List Third Party Advisory lists.debian.org text/html	MLIST [debian-lts-announce] 20190424 [SECURITY] [DLA 1762-1] systemd security update
Pony Mail!	lists.apache.org text/html	MLIST [bookkeeper-issues] 20210629 [GitHub] [bookkeeper] padma81 opened a new issue #2746: Security Vulnerabilities in CentOS 7 image, Upgrade image to CentOS 8
oss-security - Re: CVE-2017-18078: systemd-tmpfiles root privilege escalation with fs.protected_hardlinks=0	Mailing List Third Party Advisory www.openwall.com text/html	MLIST [oss-security] 20180129 Re: CVE-2017-18078: systemd-tmpfiles root privilege
openSUSE-SU-2018:0560-1: moderate: Security update for systemd	Mailing List Third Party Advisory lists.opensuse.org text/html	SUSE openSUSE-SU-2018:0560
oss-security - CVE-2018-18078: systemd-tmpfiles root privilege escalation with fs.protected_hardlinks=0	Exploit Mailing List Third Party Advisory www.openwall.com text/html	MLIST [oss-security] 20180129 CVE-2018-18078: systemd-tmpfiles root privilege escalation with fs.protected_hardlinks=0
systemd Local Privilege Escalation ≈ Packet Storm	Exploit Third Party Advisory VDB Entry packetstormsecurity.com text/html	MISC packetstormsecurity.com/files/146184/systemd-Local-Privilege-Escalation.html
Pony Mail!	lists.apache.org text/html	MLIST [bookkeeper-issues] 20210628 [GitHub] [bookkeeper] padma81 opened a new issue #2746: Security Vulnerabilities in CentOS 7 image, Upgrade image to CentOS 8
systemd (systemd-tmpfiles) < 236 - 'fs.protected_hardlinks=0' Local Privilege Escalation - Linux local Exploit	Exploit Third Party Advisory VDB Entry www.exploit-db.com Proof of Concept text/html	EXPLOIT-DB 43935

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Application	Freedesktop	Systemd	All	All	All	All

Application	Freedesktop	Systemd	All	All	All	All
Operating System	Opensuse	Leap	42.3	All	All	All
Operating System	Opensuse	Leap	42.3	All	All	All
Application	Systemd Project	Systemd	All	All	All	All

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

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

cpe:2.3:a:freedesktop:systemd:*:*:*:*:*:*:*:*:

cpe:2.3:a:freedesktop:systemd:*:*:*:*:*:*:*:*:

cpe:2.3:o:opensuse:leap:42.3:*:*:*:*:*:*:*:

cpe:2.3:o:opensuse:leap:42.3:*:*:*:*:*:*:*:

cpe:2.3:a:systemd_project:systemd:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→