Alpine Linux - Bug #9848

Bug # 9847 (Closed): tar: Infinite read loop in sparse_dump_region function in sparse.c (CVE-2018-20482)

[3.8] tar: Infinite read loop in sparse_dump_region function in sparse.c (CVE-2018-20482)

01/10/2019 12:16 PM - Alicha CH

Status:	Closed	**Start date:**	01/10/2019
Priority:	Normal	**Due date:**	
Assignee:	Carlo Landmeter	**% Done:**	100%
Category:	Security	**Estimated time:**	0.00 hour
Target version:	3.8.2		
Affected versions:		**Security IDs:**	CVE-2018-20482

Description

GNU Tar through 1.30, when --sparse is used, mishandles file shrinkage during read access, which allows local users to cause a denial of service (infinite read loop in sparse_dump_region in sparse.c) by modifying a file that is supposed to be archived by a different user's process (e.g., a system backup running as root).

References:

https://utcc.utoronto.ca/~cks/space/blog/sysadmin/TarFindingTruncateBug
https://nvd.nist.gov/vuln/detail/CVE-2018-20482

Patch:

http://git.savannah.gnu.org/cgit/tar.git/commit/?id=c15c42c

Associated revisions

Revision 0119db77 - 01/17/2019 03:19 PM - J0WI

main/tar: security upgrade to 1.31

fixes #9848

History

#1 - 01/17/2019 03:20 PM - Anonymous

- Status changed from New to Resolved

- % Done changed from 0 to 100

Applied in changeset alpine:0119db774c8cbd96f7d4d966f9fa9c2f788f223a.

#2 - 01/18/2019 02:35 PM - Alicha CH

- Project changed from Alpine Security to Alpine Linux

- Category set to Security

- Status changed from Resolved to Closed