Alpine Linux - Bug #9783

Bug # 9781 (Closed): netatalk: Unauthenticated remote code execution (CVE-2018-1160)

[3.8] netatalk: Unauthenticated remote code execution (CVE-2018-1160)

12/24/2018 11:19 AM - Alicha CH

Status:	Closed	**Start date:**	12/24/2018
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	100%
Category:	Security	**Estimated time:**	0.00 hour
Target version:	3.8.2		
Affected versions:		**Security IDs:**	CVE-2018-1160

Description

Netatalk before 3.1.12 is vulnerable to an out of bounds write in dsi_opensess.c. This is due to lack of bounds checking on attacker controlled data.
A remote unauthenticated attacker can leverage this vulnerability to achieve arbitrary code execution.

References:

http://netatalk.sourceforge.net/3.1/ReleaseNotes3.1.12.html
https://nvd.nist.gov/vuln/detail/CVE-2018-1160

Patch:

https://github.com/Netatalk/Netatalk/commit/750f9b55844b444b8ff1a38206fd2bdbab85c21f

Associated revisions

Revision f6b482c9 - 02/04/2019 01:36 PM - Leonardo Arena

community/netatalk: security upgrade to 3.1.12 (CVE-2018-1160)

Fixes #9783

History

#1 - 02/04/2019 01:36 PM - Anonymous

- Status changed from New to Resolved

- % Done changed from 0 to 100

Applied in changeset alpine:f6b482c960d38009a0ea14f0c3c494978fcc4892.

#2 - 02/19/2019 11:24 AM - Alicha CH

- Project changed from Alpine Security to Alpine Linux

- Category set to Security

- Status changed from Resolved to Closed