Alpine Linux - Bug #9499

Bug # 9497 (Closed): gd: Double free in src/gd_bump.c:gdImageBmpPtr() via crafted JPEG (CVE-2018-1000222)

[3.8] gd: Double free in src/gd_bump.c:gdImageBmpPtr() via crafted JPEG (CVE-2018-1000222)

10/02/2018 09:11 AM - Alicha CH

Status:	Closed	**Start date:**	10/02/2018
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:**	

Description

Libgd version 2.2.5 contains a Double Free Vulnerability vulnerability in gdImageBmpPtr Function that can result
in Remote Code Execution . This attack appear to be exploitable via Specially Crafted Jpeg Image can trigger double free.
This vulnerability appears to have been fixed in after commit ac16bdf2d41724b5a65255d4c28fb0ec46bc42f5.

References:

https://github.com/libgd/libgd/issues/447
https://nvd.nist.gov/vuln/detail/CVE-2018-1000222

Patch:

https://github.com/libgd/libgd/commit/ac16bdf2d41724b5a65255d4c28fb0ec46bc42f5

Associated revisions

Revision 0b188437 - 10/02/2018 02:05 PM - Natanael Copa

main/gd: backport security fix for CVE-2018-1000222

fixes #9499

History

#1 - 10/02/2018 02:06 PM - Natanael Copa

- Status changed from New to Resolved

- % Done changed from 0 to 100

Applied in changeset alpine:0b18843792bc3a090f55ce0f51d3f3049ff91f23.

#2 - 10/04/2018 10:07 AM - Alicha CH

- Project changed from Alpine Security to Alpine Linux

- Category set to Security

- Status changed from Resolved to Closed

- Security IDs deleted (CVE-2018-1000222)