Alpine Linux - Bug #9434

Bug # 9432 (Closed): ghostscript: Incorrect "restoration of privilege" checking when running out of stack during exception handling (CVE-2018-16802)

[3.8] ghostscript: Incorrect "restoration of privilege" checking when running out of stack during exception handling (CVE-2018-16802)

09/20/2018 10:41 AM - Alicha CH

Status:	Closed	**Start date:**	09/20/2018
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	100%
Category:	Security	**Estimated time:**	0.00 hour
Target version:	3.8.2		
Affected versions:		**Security IDs:**	

Description

An issue was discovered in Artifex Ghostscript before 9.25. Incorrect "restoration of privilege" checking when running out of stack during exception handling could be used by attackers able to supply crafted PostScript to execute code using the "pipe" instruction. This is due to an incomplete fix for CVE-2018-16509.

References:

https://seclists.org/oss-sec/2018/q3/228
https://seclists.org/oss-sec/2018/q3/229
https://seclists.org/oss-sec/2018/q3/233

Patches:

https://git.ghostscript.com/?p=ghostpdl.git;a=commit;h=643b24db
https://git.ghostscript.com/?p=ghostpdl.git;a=commit;h=3e5d316b
https://git.ghostscript.com/?p=ghostpdl.git;a=commit;h=5812b1b7

Associated revisions

Revision 81f78446 - 11/07/2018 07:49 AM - Leonardo Arena

main/ghostscript: security upgrade to 9.25 (CVE-2018-16802)

Fixes #9434

History

#1 - 11/07/2018 07:49 AM - Anonymous

- Status changed from New to Resolved

- % Done changed from 0 to 100

Applied in changeset alpine:81f784469ba2ef0a8d3eb4748c1ba9d6269fb430.

#2 - 11/08/2018 09:29 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-2018-16802)