Alpine Linux - Bug #9691

Bug # 9689 (Closed): ghostscript: Multiple vulnerabilities: (CVE-2018-19409, CVE-2018-19475, CVE-2018-19476, CVE-2018-19477)

[3.8] ghostscript: Multiple vulnerabilities: (CVE-2018-19409, CVE-2018-19475, CVE-2018-19476, CVE-2018-19477)

11/26/2018 02:18 PM - Alicha CH

Status:	Closed	**Start date:**	11/26/2018
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	100%
Category:	Security	**Estimated time:**	0.00 hour
Target version:	3.8.2		
Affected versions:		**Security IDs:**	CVE-2018-19409, CVE-2018-19475, CVE-2018-19476, CVE-2018-19477

Description

CVE-2018-19409: An issue was discovered in Artifex Ghostscript before 9.26. LockSafetyParams is not checked correctly if another device is used.

Fixed In Version:

ghostscript 9.26

References:

https://www.ghostscript.com/doc/9.26/History9.htm#Version9.26
https://nvd.nist.gov/vuln/detail/CVE-2018-19409

Patches:

https://git.ghostscript.com/?p=ghostpdl.git;a=commitdiff;h=661e8d8fb
https://git.ghostscript.com/?p=ghostpdl.git;a=commitdiff;h=ea1b3ef43

CVE-2018-19475: psi/zdevice2.c in Artifex Ghostscript before 9.26 allows remote attackers to bypass intended access restrictions because available stack space is not checked when the device remains the same.

References:

https://nvd.nist.gov/vuln/detail/CVE-2018-19475
https://bugs.ghostscript.com/show_bug.cgi?id=700153

Patches:

http://git.ghostscript.com/?p=ghostpdl.git;a=commit;h=3005fcb9bb160af199e761e03bc70a9f249a987e (ghostscript-9.26)
http://git.ghostscript.com/?p=ghostpdl.git;a=commit;h=aeea342904978c9fe17d85f4906a0f6fcce2d315 (master)

CVE-2018-19476: psi/zicc.c in Artifex Ghostscript before 9.26 allows remote attackers to bypass intended access restrictions because of a setcolorspace type confusion.

References:

https://nvd.nist.gov/vuln/detail/CVE-2018-19476
https://bugs.ghostscript.com/show_bug.cgi?id=700169

Patches:

http://git.ghostscript.com/?p=ghostpdl.git;a=commit;h=67d760ab775dae4efe803b5944b0439aa3c0b04a (ghostscript-9.26)
http://git.ghostscript.com/?p=ghostpdl.git;a=commit;h=434753adbe8be5534bfb9b7d91746023e8073d16 (master)

CVE-2018-19477: psi/zfjbig2.c in Artifex Ghostscript before 9.26 allows remote attackers to bypass intended access restrictions because of a JBIG2Decode type confusion.

References:

https://nvd.nist.gov/vuln/detail/CVE-2018-19477
https://bugs.ghostscript.com/show_bug.cgi?id=700168

Patches:

http://git.ghostscript.com/?p=ghostpdl.git;a=commit;h=ef252e7dc214bcbd9a2539216aab9202848602bb (ghostscript-9.26)
http://git.ghostscript.com/?p=ghostpdl.git;a=commit;h=606a22e77e7f081781e99e44644cd0119f559e03 (master)

Associated revisions

Revision 38c2fab4 - 11/29/2018 02:35 PM - J0WI

main/ghostscript: security fixes (CVE-2018-17961, CVE-2018-18073, CVE-2018-18284)

ref #9691

Revision d58edba2 - 11/29/2018 02:35 PM - Andy Postnikov

main/ghostscript: security upgrade to 9.26 (CVE-2018-19409)

fixes #9691

History

#1 - 11/28/2018 10:51 AM - Alicha CH

- Subject changed from [3.8] ghostscript: Improperly implemented security check in zsetdevice function in psi/zdevice.c (CVE-2018-19409) to [3.8] ghostscript: Multiple vulnerabilities: (CVE-2018-19409, CVE-2018-19475, CVE-2018-19476, CVE-2018-19477)

- Description updated

- Security IDs changed from CVE-2018-19409 to CVE-2018-19409, CVE-2018-19475, CVE-2018-19476, CVE-2018-19477

#2 - 11/29/2018 02:37 PM - Andy Postnikov

- Status changed from New to Resolved

- % Done changed from 0 to 100

Applied in changeset alpine:d58edba21f19cbfda556148ab655755ccde6e857.

#3 - 12/07/2018 10:51 AM - Alicha CH

- Project changed from Alpine Security to Alpine Linux

- Category set to Security

- Status changed from Resolved to Closed