Alpine Linux - Bug #6954

Bug # 6953 (Closed): gdk-pixbuf: Multiple vulnerabilities (CVE-2017-6311, CVE-2017-6312, CVE-2017-6313, CVE-2017-6314)

[3.6] gdk-pixbuf: Multiple vulnerabilities (CVE-2017-6311, CVE-2017-6312, CVE-2017-6313, CVE-2017-6314)

03/03/2017 11:10 AM - Alicha CH

Status:	Closed	**Start date:**	03/03/2017
Priority:	Normal	**Due date:**	
Assignee:	Natanael Copa	**% Done:**	100%
Category:	Security	**Estimated time:**	0.00 hour
Target version:	3.6.2		
Affected versions:		**Security IDs:**	

Description

CVE-2017-6311: NULL dereference on gdk-pixbuf thumbnailer

References:

https://bugzilla.gnome.org/show_bug.cgi?id=778204
http://seclists.org/oss-sec/2017/q1/466
http://mov.sx/2017/02/21/bug-hunting-gdk-pixbuf.html

CVE-2017-6312: Out-of-bounds read in io-ico.c

References:

https://bugzilla.gnome.org/show_bug.cgi?id=779012
http://seclists.org/oss-sec/2017/q1/466
http://mov.sx/2017/02/21/bug-hunting-gdk-pixbuf.html

CVE-2017-6313: Integer underflow in io-icns.c

References:

https://bugzilla.gnome.org/show_bug.cgi?id=779016
http://seclists.org/oss-sec/2017/q1/466
http://mov.sx/2017/02/21/bug-hunting-gdk-pixbuf.html

CVE-2017-6314: Infinite loop in io-tiff.c

References:

https://bugzilla.gnome.org/show_bug.cgi?id=779020
http://seclists.org/oss-sec/2017/q1/466
http://mov.sx/2017/02/21/bug-hunting-gdk-pixbuf.html

Associated revisions

Revision b94677ab - 06/16/2017 08:32 AM - Leonardo Arena

main/gdk-pixbuf: security fixes (CVE-2017-6311, CVE-2017-6312, CVE-2017-6314)

Partially fixes #6954

CVE-2017-6313: fix N/A, https://bugzilla.gnome.org/show_bug.cgi?id=779016

History

#1 - 04/14/2017 02:02 PM - Sergei Lukin

2.36.6 (available in AL 3.6) is already latest release atm (2017-04-14)
http://ftp.gnome.org/pub/gnome/sources/gdk-pixbuf/

Fixes for CVE-2017-6311, CVE-2017-6312, CVE-2017-6313, CVE-2017-6314 are not available

https://security-tracker.debian.org/tracker/CVE-2017-6311
https://security-tracker.debian.org/tracker/CVE-2017-6312
https://security-tracker.debian.org/tracker/CVE-2017-6313
https://security-tracker.debian.org/tracker/CVE-2017-6313

#2 - 05/25/2017 10:39 AM - Natanael Copa

- Target version changed from 3.6.0 to 3.6.1

#3 - 06/01/2017 07:19 PM - Natanael Copa

- Target version changed from 3.6.1 to 3.6.2

#4 - 06/16/2017 08:34 AM - Anonymous

- Status changed from New to Resolved

- % Done changed from 0 to 100

Applied in changeset alpine:b94677ab61788321ca49525a88ae523c9f0a6bca.

#5 - 06/29/2017 07:23 AM - Alicha CH

- Category set to Security

- Status changed from Resolved to Closed