Alpine Linux - Bug #9534

Bug # 9532 (Closed): libx11: Multiple vulnerabilities (CVE-2018-14598, CVE-2018-14599, CVE-2018-14600)

[3.8] libx11: Multiple vulnerabilities (CVE-2018-14598, CVE-2018-14599, CVE-2018-14600)

10/08/2018 11:06 AM - Alicha CH

Status:	Closed	**Start date:**	10/08/2018
Priority:	Normal	**Due date:**	
Assignee:	Natanael Copa	**% Done:**	100%
Category:	Security	**Estimated time:**	0.00 hour
Target version:	3.8.2		
Affected versions:		**Security IDs:**	

Description

CVE-2018-14598: Crash on invalid reply in XListExtensions in ListExt.c

An issue was discovered in ListExt.c:XListExtensions and GetFPath.c:XGetFontPath in libX11 through version 1.6.5. A malicious server can send
a reply in which the first string overflows, causing a variable to be set to NULL that will be freed later on, leading to DoS (segmentation fault).

Fixed In Version:

libX11 1.6.6

References:

http://www.openwall.com/lists/oss-security/2018/08/21/6
https://lists.x.org/archives/xorg-announce/2018-August/002916.html

Patch:

https://cgit.freedesktop.org/xorg/lib/libX11/commit/?id=e83722768fd5c467ef61fa159e8c6278770b45c2

CVE-2018-14599: off-by-one error in XListExtensions in ListExt.c

An issue was discovered in libX11 through 1.6.5. Functions GetFPath.c:XGetFontPath, ListExt.c:XListExtensions and FontNames.c:XListFonts are
vulnerable to an off-by-one error when parsing list of strings returned by malicious server responses, leading to DoS.

Fixed In Version:

libX11 1.6.6

References:

http://www.openwall.com/lists/oss-security/2018/08/21/6
https://lists.x.org/archives/xorg-announce/2018-August/002916.html

Patch:

https://cgit.freedesktop.org/xorg/lib/libX11/commit/?id=b469da1430cdcee06e31c6251b83aede072a1ff0

CVE-2018-14600: Out of Bounds write in XListExtensions in ListExt.c

An issue was discovered in libX11 through 1.6.5. Functions ListExt.c:XListExtensions and GetFPath.c:XGetFontPath interpret a variable as signed instead
of unsigned, resulting in an out-of-bounds write (of up to 128 bytes), leading to DoS or remote code execution.

Fixed In Version:

libX11 1.6.6

References:

http://www.openwall.com/lists/oss-security/2018/08/21/6
https://lists.x.org/archives/xorg-announce/2018-August/002916.html

Patch:

https://cgit.freedesktop.org/xorg/lib/libX11/commit/?id=dbf72805fd9d7b1846fe9a11b46f3994bfc27fea

Associated revisions

Revision d7c441ba - 10/08/2018 11:52 AM - Natanael Copa

main/libx11: security upgrade to 1.6.6

CVE-2018-14598
CVE-2018-14599
CVE-2018-14600

fixes #9534

History

#1 - 10/08/2018 11:55 AM - Natanael Copa

- Status changed from New to Resolved

- % Done changed from 0 to 100

Applied in changeset alpine:d7c441ba3f0fdfc555c09ca51f315ba46459eaa4.

#2 - 10/09/2018 06:50 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-2018-14598, CVE-2018-14599, CVE-2018-14600)