Alpine Linux - Bug #6638

Bug # 6636 (Closed): libvncserver: heap buffer overflows (CVE-2016-9941, CVE-2016-9942)

[3.5] libvncserver: heap buffer overflows (CVE-2016-9941, CVE-2016-9942)

01/06/2017 01:29 PM - Alicha CH

Status:	Closed	**Start date:**	01/06/2017
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	100%
Category:	Security	**Estimated time:**	0.00 hour
Target version:	3.5.1		
Affected versions:		**Security IDs:**	

Description

CVE-2016-9941: Heap-based buffer overflow in rfbproto.c

Heap-based buffer overflow in rfbproto.c was found in LibVNCClient in LibVNCServer before 0.9.11 that allows remote servers to cause a denial of service
(application crash) or possibly execute arbitrary code via a crafted FramebufferUpdate message containing a subrectangle outside of the client drawing area.

Fixed In Version:

libvncserver 0.9.11

Reference:

https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-9941

Patch:

https://github.com/LibVNC/libvncserver/commit/5418e8007c248bf9668d22a8c1fa9528149b69f2

CVE-2016-9942: Heap-based buffer overflow in ultra.c

Heap-based buffer overflow was found in ultra.c in LibVNCClient in LibVNCServer before 0.9.11 that allows remote servers to cause a denial of service (application crash)
or possibly execute arbitrary code via a crafted FramebufferUpdate message with the Ultra type tile, such that the LZO payload decompressed length exceeds what is specified by the tile dimensions.

Fixed In Version:

libvncserver 0.9.11

Reference:

https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-9942

Patch:

https://github.com/LibVNC/libvncserver/commit/5fff4353f66427b467eb29e5fdc1da4f2be028bb

Associated revisions

Revision 09e18065 - 01/12/2017 07:55 AM - Sergei Lukin

main/libvncserver: security fixes #6638

CVE-2016-9941: Heap-based buffer overflow in rfbproto.c
CVE-2016-9942: Heap-based buffer overflow in ultra.c

History

#1 - 01/12/2017 07:57 AM - Sergei Lukin

- Status changed from New to Resolved

- % Done changed from 0 to 100

Applied in changeset alpine:09e180651f0e822f8487bf871bcac7b44a2e383a.

#2 - 01/12/2017 02:24 PM - Natanael Copa

- Target version changed from 3.5.0 to 3.5.1

#3 - 01/23/2017 09:35 AM - Alicha CH

- Category set to Security

- Status changed from Resolved to Closed