Alpine Linux - Bug #8557

Bug # 8556 (Closed): libvncserver: Improper input sanitization in rfbProcessClientNormalMessage in rfbserver.c ((CVE-2018-7225)

[3.8] libvncserver: Improper input sanitization in rfbProcessClientNormalMessage in rfbserver.c ((CVE-2018-7225)

02/23/2018 01:56 PM - Alicha CH

Status:	Closed	**Start date:**	02/23/2018
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	100%
Category:	Security	**Estimated time:**	0.00 hour
Target version:	3.8.1		
Affected versions:		**Security IDs:**	

Description

An issue was discovered in LibVNCServer through 0.9.11. rfbProcessClientNormalMessage() in rfbserver.c does not sanitize msg.cct.length, leading to access
to uninitialized and potentially sensitive data or possibly unspecified other impact (e.g., an integer overflow) via specially crafted VNC packets.

References:

https://github.com/LibVNC/libvncserver/issues/218
http://www.openwall.com/lists/oss-security/2018/02/18/1

History

#1 - 06/26/2018 10:14 AM - Natanael Copa

- Target version changed from 3.8.0 to 3.8.1

#2 - 08/08/2018 03:40 PM - Natanael Copa

- Status changed from New to Resolved

- % Done changed from 0 to 100

fixed with alpine:8cb1ee23b7bc0d719ec7229ba43bf47891d68dbf

#3 - 08/09/2018 08:12 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-2018-7225)