Alpine Linux - Bug #9307

Bug # 9305 (Closed): spice: Missing check in demarshal.py:write_validate_array_item() allows for buffer overflow and denial of service (CVE-2018-10873)

[3.8] spice: Missing check in demarshal.py:write_validate_array_item() allows for buffer overflow and denial of service (CVE-2018-10873)

08/21/2018 10:43 AM - Alicha CH

Status:	Closed	**Start date:**	08/21/2018
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

A vulnerability was discovered in SPICE before version 0.14.1 where the generated code used for demarshalling messages lacked sufficient bounds checks. A malicious client or server, after authentication, could send specially crafted messages to its peer which would result in a crash or, potentially, other impacts.

References:

http://openwall.com/lists/oss-security/2018/08/17/1
https://nvd.nist.gov/vuln/detail/CVE-2018-10873

Patch:

https://gitlab.freedesktop.org/spice/spice-common/commit/bb15d4815ab586b4c4a20f4a565970a44824c42c

Related issues:

Copied from Alpine Linux - Bug #9305: spice: Missing check in demarshal.py:wr...	**Closed**	**08/21/2018**

Associated revisions

Revision 03fec458 - 11/07/2018 01:47 PM - Leonardo Arena

main/spice: security upgrade to 0.14.1 (CVE-2018-10873)

Fixes #9307

History

#1 - 08/21/2018 10:43 AM - Alicha CH

- Copied from Bug #9305: spice: Missing check in demarshal.py:write_validate_array_item() allows for buffer overflow and denial of service (CVE-2018-10873) added

#3 - 09/11/2018 01:49 PM - Natanael Copa

- Target version changed from 3.8.1 to 3.8.2

#4 - 11/07/2018 01:50 PM - Anonymous

- Status changed from New to Resolved

- % Done changed from 0 to 100

Applied in changeset alpine:03fec4585c1e4a7736a7727b5a03e477dbd27bab.

#5 - 11/08/2018 09:59 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-2018-10873)