Alpine Linux - Bug #9941

Bug # 9939 (Closed): spice: Off-by-one error in array access in spice/server/memslot.c (CVE-2019-3813)

[3.8] spice: Off-by-one error in array access in spice/server/memslot.c (CVE-2019-3813)

01/29/2019 02:15 PM - Alicha CH

Status:	Closed	**Start date:**	01/29/2019
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:**	CVE-2019-3813

Description

spice versions 0.5.2 through 0.14.1 are vulnerable to an out-of-bounds read due to an off-by-one error in memslot_get_virt. This may lead to a denial-of-service, or, in the worst case, code-execution by unauthenticated attackers.

Fixed In Version:

spice 0.14.2

References:

https://www.openwall.com/lists/oss-security/2019/01/28/2

Associated revisions

Revision 82adc424 - 01/31/2019 11:20 AM - Leonardo Arena

main/spice: security fix (CVE-2019-3813)

Fixes #9941

History

#1 - 01/31/2019 11:21 AM - Anonymous

- Status changed from New to Resolved

- % Done changed from 0 to 100

Applied in changeset alpine:82adc424bea28cbebf05ecf189452d69b7a82430.

#2 - 02/14/2019 09:59 AM - Alicha CH

- Project changed from Alpine Security to Alpine Linux

- Category set to Security

- Status changed from Resolved to Closed