Alpine Linux - Bug #6783

Bug # 6782 (Closed): ansible: host to controller command execution vulnerability (CVE-2016-9587)

[3.5] ansible: host to controller command execution vulnerability (CVE-2016-9587)

01/31/2017 10:49 AM - Alicha CH

Status:	Closed	**Start date:**	01/31/2017
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	100%
Category:	Security	**Estimated time:**	0.00 hour
Target version:	3.5.2		
Affected versions:		**Security IDs:**	

Description

An input validation vulnerability was found in Ansible's handling of data sent from client systems. An attacker with control over a client system being managed
by Ansible and the ability to send facts back to the Ansible server could use this flaw to execute arbitrary code on the Ansible server using the Ansible-server privileges.

Fixed in:

Ansible 2.2.1, and 2.1.4

References:

https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2016-9587
https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=850846

Associated revisions

Revision aff146eb - 02/01/2017 01:16 PM - Sergei Lukin

main/ansible: security upgrade to 2.2.1.0 - fixes #6783

CVE-2016-9587: host to controller command execution vulnerability

History

#1 - 02/01/2017 01:17 PM - Sergei Lukin

- Status changed from New to Resolved

- % Done changed from 0 to 100

Applied in changeset alpine:aff146eb533abca2d555f194246efde905e1ff40.

#2 - 02/02/2017 09:27 AM - Alicha CH

- Category set to Security

- Status changed from Resolved to Closed