Alpine Linux - Bug #6803

[3.5] salt: multiple issues (CVE-2017-5192, CVE-2017-5200)

02/02/2017 12:10 PM - Alicha CH

Status:	Closed	**Start date:**	02/02/2017
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	100%
Category:	Security	**Estimated time:**	0.00 hour
Target version:	3.5.2		
Affected versions:		**Security IDs:**	

Description

CVE-2017-5192: local_batch client external authentication not respected

The `LocalClient.cmd_batch()` method client does not accept `external_auth` credentials and so access to it from salt-api has been removed for now. This vulnerability allows code execution for already- authenticated users and is only in effect when running salt-api as the `root` user.

Fixed In Version:

salt 2015.8.13, salt 2016.3.5, **salt 2016.11.2**

Reference:

https://docs.saltstack.com/en/latest/topics/releases/2016.11.2.html

CVE-2017-5200: Salt-api allows arbitrary command execution on a salt-master via Salt's ssh_client

Users of Salt-API and salt-ssh could execute a command on
the salt master via a hole when both systems were enabled.

Fixed In Version:

salt 2015.8.13, salt 2016.3.5, **salt 2016.11.2**

Reference:

https://docs.saltstack.com/en/latest/topics/releases/2016.11.2.html

Associated revisions

Revision e8237cd8 - 02/06/2017 09:19 AM - Sergei Lukin

community/salt: security upgrade to 2016.11.2 - fixes #6803

CVE-2017-5192: local_batch client external authentication not respected
CVE-2017-5200: Salt-api allows arbitrary command execution on a salt-master via Salt's ssh_client

History

#1 - 02/06/2017 09:19 AM - Sergei Lukin

- Status changed from New to Resolved

- % Done changed from 0 to 100

Applied in changeset alpine:e8237cd8d1322e86e07ad29fc835c0d356ba2aa6.

#2 - 02/06/2017 10:20 AM - Alicha CH

- Project changed from Alpine Security to Alpine Linux

- Category set to Security

- Status changed from Resolved to Closed