Alpine Linux - Bug #6943

[3.5] shadow: Several vulnerabilities (CVE-2016-6252, CVE-2017-2616)

02/27/2017 12:43 PM - Alicha CH

Status:	Closed	**Start date:**	02/27/2017
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-2016-6252: Integer overflow in shadow 4.2.1 allows local users to gain privileges via crafted input to newuidmap.

References:

https://github.com/shadow-maint/shadow/issues/27
http://seclists.org/oss-sec/2016/q3/115

Patch:

https://github.com/shadow-maint/shadow/commit/1d5a926cc2d6078d23a96222b1ef3e558724dad1

CVE-2017-2616: su: properly clear child PID

Reference:

https://security-tracker.debian.org/tracker/CVE-2017-2616

Patch:

https://github.com/shadow-maint/shadow/commit/08fd4b69e84364677a10e519ccb25b71710ee686

Both patches were added to git master:
http://git.alpinelinux.org/cgit/aports/commit/community/shadow?id=e9a92d060e2e59ac087373af9b81546c2a761d07

Associated revisions

Revision 0d877346 - 02/28/2017 02:40 PM - Henrik Riomar

community/shadow: CVE-2016-6252 & CVE-2017-2616

Patches from Debian Jessie (1:4.2-3+deb8u3 & 1:4.2-3+deb8u2)

fixes #6943

(cherry picked from commit e9a92d060e2e59ac087373af9b81546c2a761d07)

History

#1 - 02/28/2017 02:41 PM - Henrik Riomar

- Status changed from New to Resolved

- % Done changed from 0 to 100

Applied in changeset alpine:0d87734696c2c04083fae90ef045d87926d35ebd.

#2 - 03/03/2017 09:23 AM - Alicha CH

- Project changed from Alpine Security to Alpine Linux

- Category set to Security

- Status changed from Resolved to Closed