Alpine Linux - Bug #6655

Bug # 6653 (Closed): bash: popd controlled free (CVE-2016-9401)

[3.5] bash:popd controlled free (CVE-2016-9401)

01/10/2017 08:22 AM - Alicha CH

Status:	Closed	**Start date:**	01/10/2017
Priority:	Normal	**Due date:**	
Assignee:	Natanael Copa	**% Done:**	100%
Category:	Security	**Estimated time:**	0.00 hour
Target version:	3.5.1		
Affected versions:		**Security IDs:**	

Description

A vulnerability was found in popd. It can be tricked to free a user supplied address in the following way:

$ popd +-111111

This could be used to bypass restricted shells (rsh) on some environments to cause use-after-free.

Reference:

https://lists.gnu.org/archive/html/bug-bash/2016-11/msg00099.html
http://seclists.org/oss-sec/2016/q4/445

Patch:

https://lists.gnu.org/archive/html/bug-bash/2016-11/msg00116.html

Associated revisions

Revision 88fc2ef0 - 01/24/2017 09:22 AM - Sergei Lukin

main/bash: security fixes #6655

CVE-2016-9401

History

#1 - 01/12/2017 02:23 PM - Natanael Copa

- Target version changed from 3.5.0 to 3.5.1

#2 - 01/24/2017 10:08 AM - Sergei Lukin

- Status changed from New to Resolved

- % Done changed from 0 to 100

Applied in changeset alpine:88fc2ef0acfc8d5519e18e4f1965ab42eb7243b2.

#3 - 01/25/2017 09:44 AM - Alicha CH

- Category set to Security

- Status changed from Resolved to Closed