Alpine Linux - Bug #6672

[3.5] docker: insecure opening of file-descriptor allows privilege escalation (CVE-2016-9962)

01/12/2017 02:08 PM - Alicha CH

Status:	Closed	**Start date:**	01/12/2017
Priority:	Normal	**Due date:**	
Assignee:	Eivind Uggedal	**% Done:**	100%
Category:	Security	**Estimated time:**	0.00 hour
Target version:	3.5.1		
Affected versions:		**Security IDs:**	

Description

RunC allowed additional container processes via `runc exec` to be ptraced by the pid 1 of the container.
This allows the main processes of the container, if running as root, to gain access to file-descriptors of these new
processes during the initialization and can lead to container escapes or modification of runC state before the process is fully placed inside the container.

Fixed In Version:

docker 1.12.6

Reference:

http://seclists.org/oss-sec/2017/q1/54

Associated revisions

Revision 73e309f3 - 01/12/2017 03:30 PM - Natanael Copa

community/docker: security upgrade to 1.12.6 (CVE-2016-9962)

fixes #6672

History

#1 - 01/12/2017 02:21 PM - Natanael Copa

- Target version changed from 3.5.0 to 3.5.1

#2 - 01/12/2017 03:31 PM - Natanael Copa

- Status changed from New to Resolved

- % Done changed from 0 to 100

Applied in changeset alpine:73e309f355eea69de5252d2729b5373e0b12ab9a.

#3 - 01/18/2017 08:51 AM - Alicha CH

- Project changed from Alpine Security to Alpine Linux

- Category set to Security

- Status changed from Resolved to Closed