Alpine Linux - Bug #6730

Bug # 6728 (Closed): Screen: root exploit 4.5.0

[3.5] Screen: root exploit 4.5.0 (CVE-2017-5618)

01/25/2017 09:23 AM - Alicha CH

Status:	Closed	**Start date:**	01/25/2017
Priority:	Normal	**Due date:**	
Assignee:	Natanael Copa	**% Done:**	100%
Category:	Security	**Estimated time:**	0.00 hour
Target version:	3.5.2		
Affected versions:		**Security IDs:**	

Description

Commit f86a374 ("screen.c: adding permissions check for the logfile name", 2015-11-04)

The check opens the logfile with full root privileges. This allows us to
truncate any file or create a root-owned file with any contents in any
directory and can be easily exploited to full root access in several ways.

Affects:

screen 4.4.0 to and inclusive 4.5.0

References:

http://www.openwall.com/lists/oss-security/2017/01/24/10
http://savannah.gnu.org/bugs/?50142

Associated revisions

Revision 62ff75ac - 03/01/2017 05:56 PM - Natanael Copa

main/screen: security upgrade to 4.5.1 (CVE-2017-5618)

fixes #6730

History

#1 - 01/26/2017 09:56 AM - Sergei Lukin

At this moment (2017-01-26)
fix-patch is not available
CVE is not assigned for this issue
4.5.1 release was promised which would fix the issue
https://lists.gnu.org/archive/html/screen-devel/2017-01/msg00029.html
https://lists.gnu.org/archive/html/screen-devel/2017-01/msg00030.html

#2 - 01/26/2017 08:47 PM - Natanael Copa

- Target version changed from 3.5.1 to 3.5.2

#3 - 03/01/2017 05:54 PM - Natanael Copa

- Subject changed from [3.5] Screen: root exploit 4.5.0 to [3.5] Screen: root exploit 4.5.0 (CVE-2017-5618)

- Security IDs changed from - to CVE-2017-5618

#4 - 03/01/2017 05:56 PM - Natanael Copa

- Status changed from New to Resolved

- % Done changed from 0 to 100

Applied in changeset alpine:62ff75ac828e5f41d65a7b1b4785771a46f6107d.

#5 - 03/02/2017 09:09 AM - Alicha CH

- Category set to Security

- Status changed from Resolved to Closed