Alpine Linux - Bug #9824

Bug # 9822 (Closed): keepalived: Multiple vulnerabilities (CVE-2018-19044, CVE-2018-19045, CVE-2018-19046)

[3.8] keepalived: Multiple vulnerabilities (CVE-2018-19044, CVE-2018-19045, CVE-2018-19046)

01/02/2019 08:56 AM - Alicha CH

Status:	Closed	**Start date:**	01/02/2019
Priority:	Normal	**Due date:**	
Assignee:	Natanael Copa	**% Done:**	100%
Category:	Security	**Estimated time:**	0.00 hour
Target version:	3.8.2		
Affected versions:		**Security IDs:**	CVE-2018-19044, CVE-2018-19045, CVE-2018-19046

Description

CVE-2018-19044: kkeepalived before version 2.0.9 didn't check for pathnames with symlinks when writing data to a temporary file upon a call to PrintData or PrintStats. This allowed local users to overwrite arbitrary files if fs.protected_symlinks is set to 0, as demonstrated by a symlink from /tmp/keepalived.data or /tmp/keepalived.stats to /etc/passwd.

Fixed In Version:

keepalived 2.0.9

References:

https://github.com/acassen/keepalived/issues/1048
http://www.keepalived.org/changelog.html

Patch:

https://github.com/acassen/keepalived/commit/04f2d32871bb3b11d7dc024039952f2fe2750306

CVE-2018-19045: keepalived 2.0.8 used mode 0666 when creating new temporary files upon a call to PrintData or PrintStats, potentially leaking sensitive information.

Fixed In Version:

keepalived 2.0.9

References:

https://github.com/acassen/keepalived/issues/1048
https://nvd.nist.gov/vuln/detail/CVE-2018-19045

Patches:

https://github.com/acassen/keepalived/commit/5241e4d7b177d0b6f073cfc9ed5444bf51ec89d6
https://github.com/acassen/keepalived/commit/c6247a9ef2c7b33244ab1d3aa5d629ec49f0a067

CVE-2018-19046: keepalived before version 2.0.10 didn't check for existing plain files when writing data to a temporary file upon a call to PrintData or PrintStats. If a local attacker had previously created a file with the expected name (e.g., /tmp/keepalived.data or /tmp/keepalived.stats), with read access for the attacker and write access for the keepalived process, then this potentially leaked sensitive information.

Fixed In Version:

keepalived 2.0.10

References:

https://nvd.nist.gov/vuln/detail/CVE-2018-19046

https://github.com/acassen/keepalived/issues/1048

Patches:

https://github.com/acassen/keepalived/commit/ac8e2ef053de273ce7a0cf0cb611e599dca4b298
https://github.com/acassen/keepalived/commit/26c8d6374db33bcfcdcd758b1282f12ceef4b94f
https://github.com/acassen/keepalived/commit/17f944144b3d9c5131569b1cc988cc90fd676671

Associated revisions

Revision b0db67a5 - 01/08/2019 11:06 AM - Leonardo Arena

community/keepalived: security upgrade to 2.0.11

CVE-2018-19044, CVE-2018-19045, CVE-2018-19046

Fixes #9824

History

#1 - 01/08/2019 11:06 AM - Anonymous

- Status changed from New to Resolved

- % Done changed from 0 to 100

Applied in changeset alpine:b0db67a5a9a6e1d6299a426bcbbb56da356da370.

#2 - 01/09/2019 07:09 AM - Alicha CH

- Project changed from Alpine Security to Alpine Linux

- Category set to Security

- Status changed from Resolved to Closed