Alpine Linux - Bug #9998

Bug # 9995 (Closed): openssh: Multiple vulnerabilities (CVE-2018-20685, CVE-2019-6109, CVE-2019-6111)

[3.8] openssh: Multiple vulnerabilities (CVE-2018-20685, CVE-2019-6109, CVE-2019-6111)

02/20/2019 12:11 PM - Alicha CH

Status:	Closed	**Start date:**	02/20/2019
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-2018-20685, CVE-2019-6109, CVE-2019-6111

Description

CVE-2018-20685: In OpenSSH 7.9, scp.c in the scp client allows remote SSH servers to bypass intended access restrictions via the filename of . or an empty filename. The impact is modifying the permissions of the target directory on the client side.

References:

https://nvd.nist.gov/vuln/detail/CVE-2018-20685
https://marc.info/?l=oss-security&m=154745764812881&w=2

Patch:

https://github.com/openssh/openssh-portable/commit/6010c0303a422a9c5fa8860c061bf7105eb7f8b2

CVE-2019-6109: An issue was discovered in OpenSSH 7.9. Due to missing character encoding in the progress display, a malicious server (or Man-in-The-Middle attacker) can employ crafted object names to manipulate the client output, e.g., by using ANSI control codes to hide additional files being transferred. This affects refresh_progress_meter() in progressmeter.c.

References:

https://nvd.nist.gov/vuln/detail/CVE-2019-6109
https://sintonen.fi/advisories/scp-client-multiple-vulnerabilities.txt

Patch:

https://github.com/openssh/openssh-portable/commit/8976f1c4b2721c26e878151f52bdf346dfe2d54c
possibly additionally needed: https://github.com/openssh/openssh-portable/commit/bdc6c63c80b55bcbaa66b5fde31c1cb1d09a41eb

CVE-2019-6111: An issue was discovered in OpenSSH 7.9. Due to the scp implementation being derived from 1983 rcp, the server chooses which files/directories are sent to the client. However, the scp client only performs cursory validation of the object name returned (only directory traversal attacks are prevented). A malicious scp server (or Man-in-The-Middle attacker) can overwrite arbitrary files in the scp client target directory. If recursive operation (-r) is performed, the server can manipulate subdirectories as well (for example, to overwrite the .ssh/authorized_keys file).

References:

https://nvd.nist.gov/vuln/detail/CVE-2019-6111

Patch:

https://github.com/openssh/openssh-portable/commit/391ffc4b9d31fa1f4ad566499fef9176ff8a07dc

Associated revisions

Revision 6df59aea - 03/04/2019 11:21 AM - Leonardo Arena

main/openssh: security fixes

CVE-2018-20685, CVE-2019-6109, CVE-2019-6111

Rebase HPN patch

fixes #9998

History

#1 - 03/04/2019 11:22 AM - Anonymous

- Status changed from New to Resolved

- % Done changed from 0 to 100

Applied in changeset alpine:6df59aea4486cca6f0c089f72e404ee097b49a02.

#2 - 03/05/2019 07:51 AM - Alicha CH

- Project changed from Alpine Security to Alpine Linux

- Category set to Security

- Status changed from Resolved to Closed