OPENSSH SCP – MITM ATTACKS

PUBLISHED: OCTOBER 31, 2022 | LAST UPDATE: OCTOBER 31, 2022

Summary

From 2018 - 2020, several vulnerabilities were disclosed that could expose OpenSSH SCP clients to attacks by Man-in-the-Middle (MITM) and/or malicious SCP servers. These vulnerabilities could affect SCP file transfer operations initiated from the management of ACOS devices and are addressed in this document.

Item #	Vulnerability ID	Score Source	Score	Summary
1	CVE-2020-14145	CVSSv3	5.9 Med	openssh: Observable discrepancy leading to an information leak in the algorithm negotiation [1]
2	CVE-2019-6111	CVSSv3	5.9 Med	openssh: Improper validation of object names allows malicious server to overwrite files via scp client [2]
3	CVE-2019-6110	CVSSv3	6.8 Med	openssh: Acceptance and display of arbitrary stderr allows for spoofing of scp client output [3]
4	CVE-2019-6109	CVSSv3	6.8 Med	openssh: Missing character encoding in progress display allows for spoofing of scp client output [4]
5	CVE-2018-20685	CVSSv3	5.3 Med	openssh: scp client improper directory name validation [5]

Affected Releases

The table below indicates releases of ACOS exposed to this vulnerability and ACOS releases that address them. ACOS release families not indicated below are unaffected by these vulnerabilities.

Customers using affected ACOS releases can overcome vulnerability exposures by updating to the indicated resolved release. If the table does not list a corresponding resolved or unaffected release, then no ACOS release update is currently available.

Releases Affected			Releases Resolved or Unaffected
5.1.0	–	5.2.1-Px	None
5.0.1-TPS	–	5.0.2-TPS-Px	None
4.1.4-GR1	–	4.1.4-GR1-Px	None
3.2.5	–	3.2.5-Px	None

Workarounds and Mitigations

These vulnerabilities involve malicious or MITM SCP servers for exploitation. Manage and configure ACOS devices for SCP file transfer operations only with trusted SCP servers on trusted communication channels.

Alternately, manage and configure ACOS devices for file transfer operations using methods other than SCP. Other ACOS secure file transfer methods available include SFTP and HTTPS, which are not exposed to these vulnerabilities.

Software Updates

Software updates that address these vulnerabilities are or will be published at the following URL:

https://support.a10networks.com/

Vulnerability Details

The following table shares brief descriptions for the vulnerabilities addressed in this document.

Vulnerability ID	Description
CVE-2020-14145	The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.
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).
CVE-2019-6110	In OpenSSH 7.9, due to accepting and displaying arbitrary stderr output from the server, a malicious server (or Man-in-The-Middle attacker) can manipulate the client output, for example to use ANSI control codes to hide additional files being transferred.
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.
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.

Related Links

Ref #	General Link
[1]	NIST NVD, CVE-2020-14145
[2]	NIST NVD, CVE-2019-6111
[3]	NIST NVD, CVE-2019-6110
[4]	NIST NVD, CVE-2019-6109
[5]	NIST NVD, CVE-2018-20685

Acknowledgements

None

Modification History

Revision	Date	Description
1.0	2022-10-31	Initial Publication

This document is provided on an "AS IS" basis and does not imply any kind of guarantee or warranty, including the warranties of merchantability, non-infringement or fitness for a particular use. Your use of the information in this document or materials linked from this document is at your own risk. A10 Networks, Inc. reserves the right to change or update the information in this document at any time.