OPENSSH SCP – CVE-2020-15778

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

Summary

In July 2020, a vulnerability was disclosed that could allow an SCP client's user to run arbitrary commands on a remote SCP server. This vulnerability could be used by a malicious ACOS administrator to impact SCP servers.

Item #	Vulnerability ID	Score Source	Score	Summary
1	CVE-2020-15778	CVSSv3	7.8 High	openssh: scp allows command injection when using backtick characters in the destination argument [1]

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

To mitigate this vulnerability, ensure that administrative access to ACOS devices is limited to only trusted administrators.

If needed, an additional mitigation can be to ensure communication between ACOS devices and SCP servers is secured via local or network firewalls which are configured to block SCP connections from the ACOS devices. Since this will block SCP file transfers from the ACOS device, use alternate secure file transfer methods when managing and configuring these devices. Other ACOS secure file transfer methods available include SFTP and HTTPS, which are not exposed to this vulnerability.

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-2020-15778	** DISPUTED ** scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of "anomalous argument transfers" because that could "stand a great chance of breaking existing workflows."

Related Links

Ref #	General Link
[1]	NIST NVD, CVE-2020-15778

Acknowledgements

None

Modification History

Revision	Date	Description
1.0	2022-10-31	Initial Publication