Security Advisory

SSH - CVE-2016-0777

PUBLISHED: JULY 22, 2018 | LAST UPDATE: JULY 22, 2018

SUMMARY

In January 2016, openssh.org released a security advisory [1] detailing several security issues. The following vulnerabilities that may affect the TLS/SSL management plane of ACOS devices reported in that advisory are addressed in this document.

Item		Score		
#	Vulnerability ID	Source	Score	Summary
1	CVE-2016-0777	CVSS 3.0	6.5 Med	OpenSSH: Client Information leak due to use of roaming connection feature [2]

AFFECTED RELEASES

The table below indicates releases of ACOS exposed to these vulnerabilities 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
2.8.2	–	2.8.2-P7	4.1.2, 4.1.4
2.7.2	–	2.7.2-P11	4.1.0, 4.1.1, 4.1.2, 4.1.4
2.7.1	–	2.7.1-GR1-Px	4.1.0, 4.1.1, 4.1.2, 4.1.4
2.6.1-GR1	–	2.6.1-GR1-P16	4.1.0, 4.1.1, 4.1.2, 4.1.4

WORKAROUNDS AND MITIGATIONS

Common security best practices in the industry for network appliance management and control planes can enhance protection against remote malicious attacks. Limit the exploitable attack surface for critical, infrastructure, networking equipment through the use of access lists or firewall filters to and from only trusted, administrative networks or hosts.

SOFTWARE UPDATES

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

http://www.a10networks.com/support/axseries/software-downloads

VULNERABILITY DETAILS

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

Vulnerability ID	Description
CVE-2016-0777	The resend_bytes function in roaming_common.c in the client in OpenSSH 5.x, 6.x, and 7.x before 7.1p2 allows remote servers to obtain sensitive information from process memory by requesting transmission of an entire buffer, as demonstrated by reading a private key.

RELATED LINKS

Ref #	General Link
[1]	http://www.openssh.com/txt/release-7.1p2
[2]	NIST NVD, CVE-2016-0777

ACKNOWLEDGEMENTS

None

MODIFICATION HISTORY

Revision	Date	Description
1.0	2018-07-22	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.