Security Advisory

SSH - CVE-2018-15473

PUBLISHED: OCTOBER 11, 2018 | LAST UPDATE: JULY 23, 2021

SUMMARY

An OpenSSH vulnerability could allow an unauthenticated, remote attacker to determine whether given usernames exist or not on the server. No further information is disclosed and there is no potential impact to availability or integrity. This vulnerability may affect the SSH management plane service of ACOS devices and is addressed in this document.

Item		Score		
#	Vulnerability ID	Source	Score	Summary
1	CVE-2018-15473	CVSS 3.0	5.3 Med	openssh: User enumeration via malformed packets in authentication requests [1]

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
4.1.4	–	4.1.4-GR1	4.1.4-GR1-P1, 5.1.0, 5.2.0
4.1.2	–	4.1.2-P4	4.1.2-P5
4.1.1	–	4.1.1-P9	4.1.1-P10
4.1.100	–	4.1.100-P5	4.1.100-P5-SP1
4.1.0	–	4.1.0-P11	4.1.0-P12
3.2.5	–	3.2.5-P5	3.2.5-P6, 5.0.1, 5.0.2
3.2.4	–	3.2.4-P1	3.2.4-P2
3.2.3	–	3.2.3-P5	3.2.3-P6
3.2.2	–	3.2.2-P7	3.2.2-P8
2.8.2	–	2.8.2-Px	4.1.2-P5
2.7.2	–	2.7.2-Px	4.1.0-P12, 4.1.1-P10, 4.1.2-P5, 4.1.4-GR1-P1
2.7.1	–	2.7.1-GR1-Px	4.1.0-P12, 4.1.1-P10, 4.1.2-P5, 4.1.4-GR1-P1
2.6.1-GR1	–	2.6.1-GR1-P16	4.1.0-P12, 4.1.1-P10, 4.1.2-P5, 4.1.4-GR1-P1

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-2018-15473	OpenSSH through 7.7 is prone to a user enumeration vulnerability due to not delaying bailout for an invalid authenticating user until after the packet containing the request has been fully parsed, related to auth2-gss.c, auth2-hostbased.c, and auth2-pubkey.c.

RELATED LINKS

Ref #	General Link
[1]	NIST NVD, CVE-2018-15473

ACKNOWLEDGEMENTS

None

MODIFICATION HISTORY

Revision	Date	Description
1.0	2018-10-11	Initial Publication
2.0	2019-08-05	Updated affected and resolved releases for 4.1.4-GR1 and 3.x ACOS release families, including addition of 3.2.4 release family.
3.0	2019-10-11	Added 4.1.100 release familiy
4.0	2021-07-23	Added 3.2.5, 5.0.1, 5.0.2, 5.1.0, 5.2.0 release families

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.