SSH - SHA2 HMACS, CVE-2008-5161, WEAK MACS

PUBLISHED: AUGUST 8, 2017 | LAST UPDATE: MAY 30, 2018

SUMMARY

The SSH, remote access service of the ACOS management interface include support for weak ciphers and MAC algorithms. Accordingly, the following vulnerabilities are addressed in this document.

Item #	Vulnerability ID	Score Source	Score	Summary
1	A10-2017-0001 [a]	A10	n/a	SSH - SHA2 HMACs for stronger security
2	CVE-2008-5161	CVSS 2.0	2.6 Low	SSH Server CBC Mode Ciphers Enabled [2]
3	71049	Nessus	2.6 Low	SSH Weak MAC Algorithms Enabled [1]
4	70658	Nessus	2.6 Low	SSH Server CBC Mode Ciphers Enabled [3]

[a] A10 Networks, Inc. assigned identifier.

AFFECTED RELEASES

The table below indicates releases of ACOS exposed to these vulnerabilities and ACOS releases that address these issues or are otherwise unaffected by them.

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
4.1.2			4.1.2-P1
4.1.1	–	4.1.1-P1	4.1.1-P2
4.1.0	–	4.1.0-P8	4.1.0-P9
3.1.0-P1	–	3.2.1-P1	3.2.2-P1
2.8.2	–	2.8.2-P7	2.8.2-P8
2.7.2	–	2.7.2-P11	2.7.2-P12
2.7.1	–	2.7.1-GR1-Px	2.7.2-P12, 4.1.0-P9, 4.1.1-P2
2.6.1-GR1	–	2.6.1-GR1-P16	2.7.2-P12, 4.1.0-P9, 4.1.1-P2

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
A10-2017-0001	The remote SSH server is configured to allow additionally support SHA2 HMACs for improved security and increased compatibility with contemporary security profiles.
CVE-2008-5161	Error handling in the SSH protocol in (1) SSH Tectia Client and Server and Connector 4.0 through 4.4.11, 5.0 through 5.2.4, and 5.3 through 5.3.8; Client and Server and ConnectSecure 6.0 through 6.0.4; Server for Linux on IBM System z 6.0.4; Server for IBM z/OS 5.5.1 and earlier, 6.0.0, and 6.0.1; and Client 4.0-J through 4.3.3-J and 4.0-K through 4.3.10-K; and (2) OpenSSH 4.7p1 and possibly other versions, when using a block cipher algorithm in Cipher Block Chaining (CBC) mode, makes it easier for remote attackers to recover certain plaintext data from an arbitrary block of ciphertext in an SSH session via unknown vectors.
71049	The remote SSH server is configured to allow either MD5 or 96-bit MAC algorithms, both of which are considered weak.
70658	The SSH server is configured to support Cipher Block Chaining (CBC) encryption. This may allow an attacker to recover the plaintext message from the ciphertext.

RELATED LINKS

Ref #	General Link
[1]	Nessus: SSH Weak MAC Algorithms Enabled
[2]	NIST NVD, CVE-2008-5161
[3]	Nessus: SSH Server CBC Mode Ciphers Enabled

ACKNOWLEDGEMENTS

None

MODIFICATION HISTORY

Revision	Date	Description
1.0	2017-08-08	Initial Publication
2.0	2018-03-09	Updated release information for ACOS 4.1.1. Corrected resolved release for ACOS 2.7.2.
3.0	2018-03-19	Added missing Nessus ID (70658), incl. description and related link.
4.0	2018-05-28	Added 2.7.2-P12 as resolved/unaffected release for ACOS 2.7.1 and 2.6.1 release families.
5.0	2018-05-30	Updated 2.7.1-GR1 affected releases