SSH – NON-UNIQUE SSH HOST KEY

PUBLISHED: NOVEMBER 6, 2019 | LAST UPDATE: NOVEMBER 6, 2019

SUMMARY

Multiple ACOS release families use hardcoded SSH host keys to support SSH management access for ACOS systems. A remote attacker could exploit this vulnerability to conduct man-in-the-middle attacks by leveraging knowledge of these keys from other ACOS installations to decrypt confidential information on ACOS remote, CLI management connections.

An affected A10 system is only exposed to exploitation of this vulnerability if it is configured to use the system's default, SSH host key; without the SSH host key having been previously regenerated for the system. The following vulnerability items are addressed in this document.

Item #	Vulnerability ID	Score Source	Score	Summary
1	A10-2018-0016	CVSS 3.0	5.9 Medium	Non-Unique ACOS SSH Mgmt Host Key

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 [a]			Releases Resolved or Unaffected
3.1.0	–	3.1.4-Px	3.2.2, 3.2.3, 3.2.4 [c]
2.8.2	–	2.8.2-P9	2.8.2-P10 [b], 4.1.2, 4.1.4-GR1, 5.0.0 [c]
2.7.2	–	2.7.2-P11	2.7.2-P12 [b], 4.1.0, 4.1.1, 4.1.4-GR1, 5.0.0 [c]
2.7.1-GR1	–	2.7.1-GR1-Px	2.7.2-P12 [b], 4.1.0, 4.1.1, 4.1.4-GR1, 5.0.0 [c]
2.6.1-GR1	–	2.6.1-GR1-Px	2.7.2-P12 [b], 4.1.0, 4.1.1, 4.1.4-GR1, 5.0.0 [c]

[a] A10 systems manufactured with ACOS versions including and after 2.7.2-P12, 2.8.2-P10, and 3.2.2 are unaffected by this vulnerability; even if they have been downgraded to an affected ACOS versions

[b] Upgrading an affected A10 system to 2.7.2-P12 or 2.8.2-P10 will remediate this vulnerability, with no further actions required.

[c] Upgrading an affected A10 system to ACOS 3.2.x, 4.1.x, 5.0.0, or later release families will necessitate regeneration of the SSH host key to enable the updated and unique host key on the A10 device. Regenerating the SSH host key prior to the upgrade is recommended, by issuing the "`sshd key regenerate`" CLI command.

WORKAROUNDS AND MITIGATIONS

Regenerate the SSH host key on the ACOS system to overcome exposure to this vulnerability. The SSH host key for remote CLI management services can be regenerated by:

1. issuing the "`sshd key regenerate`" the ACOS CLI command

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
A10-2018-0016	ACOS 3.1.x, 2.8.2, 2.7.2, 2.7.1-GR1, and 2.6.1-GR1 use non-unique SSH host keys, which might allow remote attackers to defeat cryptographic protection mechanisms and conduct man-in-the-middle attacks by leveraging knowledge of these keys from another installation.

RELATED LINKS

Ref #	General Link
[1]	CERT CC Vulnerability Note - VU#566724

ACKNOWLEDGEMENTS

None

MODIFICATION HISTORY

Revision	Date	Description
1.0	2019-11-06	Initial Publication