GUI/AXAPI – NON-UNIQUE X.509 CERTIFICATE/KEY

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

SUMMARY

Multiple ACOS release families use hardcoded X.509 certificates and private keys to support HTTPS management access for ACOS systems. A remote attacker could exploit this vulnerability to conduct man-in-the-middle attacks by leveraging knowledge of these certificates and keys from other ACOS installations to decrypt confidential information on ACOS GUI and AXAPI connections.

An ACOS system with an affected release is only exposed to exploitation of this vulnerability if it is configured to use the system's default, self-signed web certificate and private-key; without having installed (uploaded) valid web credentials to the system. The following vulnerability items are addressed in this document.

Item #	Vulnerability ID	Score Source	Score	Summary
1	A10-2018-0015	CVSS 3.0	5.9 Medium	Non-Unique ACOS HTTPS Mgmt X.509 Certificate/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 [d]
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 [d]
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 [d]
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 [d]

[a] A10 systems manufactured with ACOS versions including and after 2.7.2-P12, 2.8.2-P10, and 3.1.4-Px are unaffected by this vulnerability; even if they have been downgraded to an affected ACOS version.

[b] After completing the update of an affected A10 system to 2.7.2-P12, 2.8.2-P10, or a later ACOS 2.x version, navigate to the "*Select Config Mode > System > Settings > Web Certificate*" Web/GUI page. If the certificate type indicates "*Default*", then click the "*Reset to Default*" button to enable the updated and unique default web credentials on the A10 device.

[c] After completing the update of an affected A10 system to 3.2.x, observe the certificate of the system in a browser. If the "Issuer:" field of the certificate indicates "*CN = CA_ade6dc0a8560f0a946b395e9cf08753c0eed3b14*", then issue "`web-service secure wipe`" followed by "`web-service secure restart`" CLI commands to enable the updated and unique default web credentials on the A10 device.

[d] Before upgrading an affected A10 system to ACOS 4.x or 5.x, observe the certificate of the system in a browser to determine if it is an administrator generated certificate for your organization is configured for the A10 device. If the system's web credentials were indeed uploaded and configured for the system, they could be lost in the upgrade process. After upgrading to ACOS 4.x or 5.x, verify that the certificate is unchanged. If the certificate is different, then re-uploaded the previously generated credentials or upload newly generated credentials for your organization to the A10 device using the "*System > Settings > Certificate*" Web/GUI page.

WORKAROUNDS AND MITIGATIONS

Installing unique and trusted web credentials on the ACOS system will overcome exposure to this vulnerability.

For ACOS 2.x and 3.1.x, the X.509 certificate and key for web management services can be imported using the ACOS Web/GUI page at "*Select Config Mode > System > Settings > Web Certificate*".

Administrators who subsequently issue the "`web-service certificate-reset`" ACOS CLI command will effectively restore the non-unique X.509 certificate and key. Accordingly, they will need to repeat their procedure above to ensure that the factory default certificate and key are not being used for the ACOS system.

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
A10-2018-0015	ACOS 3.1.x, 2.8.2, 2.7.2, 2.7.1-GR1, and 2.6.1-GR1 can use default, non-unique, X.509 certificate/key pair. This may allow remote attackers to defeat cryptographic protection mechanisms and conduct man-in-the-middle attacks by leveraging knowledge of these certificates and 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