SSH DH MODULUS <= 1024 BITS (LOGJAM)

PUBLISHED: JULY 14, 2018 | LAST UPDATE: OCTOBER 17, 2019

SUMMARY

The ACOS SSH server allows connections with one or more Diffie-Hellman moduli less than or equal to 1024 bits. Through cryptanalysis, a third party can find the shared secret in a short amount of time (depending on modulus size and attacker resources). This allows an attacker to recover the plaintext or potentially violate the integrity of connections.

This is the same issue as for SSL/TLS in CVE-2015-4000 (Logjam), but for SSH in this case.

Item #	Vulnerability ID	Score Source	Score	Summary
1	CVE-2015-4000	CVSS 3.0	3.7 Low	SSH Diffie-Hellman Modulus <= 1024 Bits (Logjam)

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
4.1.1	–	4.1.1-P1	4.1.1-P2
4.1.100	–	4.1.100-P5-SP1	4.1.100-P6
4.1.0	–	4.1.0-P10	4.1.0-P11
3.1.0-P1	–	3.2.2-P3	3.2.2-P4
2.8.2	–	2.8.2-Px	4.1.2
2.7.2	–	2.7.2-Px	4.1.0-P11, 4.1.1-P2, 4.1.4
2.7.1	–	2.7.1-GR1-Px	4.1.0-P11, 4.1.1-P2, 4.1.4
2.6.1-GR1	–	2.6.1-GR1-P16	4.1.0-P11, 4.1.1-P2, 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-2015-4000	The ACOS SSH server allows connections with one or more Diffie-Hellman moduli less than or equal to 1024 bits. Through cryptanalysis, a third party can find the shared secret in a short amount of time (depending on modulus size and attacker resources). This allows an attacker to recover the plaintext or potentially violate the integrity of connections. This is the issue as for SSL/TLS in CVE-2015-4000 (Logjam), but for SSH in this case.

RELATED LINKS

Ref #	General Link
[1]	Logjam: TLS vulnerabilities (CVE-2015-4000)
[2]	NIST NVD, CVE-2015-4000
[3]	SSH Diffie-Hellman Modulus <= 1024 Bits (Logjam)

ACKNOWLEDGEMENTS

None

MODIFICATION HISTORY

Revision	Date	Description
1.0	2018-07-14	Initial Publication
2.0	2018-07-18	Corrected ACOS 3.x affected release.
3.0	2019-10-17	Added 4.1.100 release family.