TLS/SSL - CVE-2016-8610

PUBLISHED: JULY 25, 2017 | LAST UPDATE: JULY 25, 2017

SUMMARY

A Denial-of-Service (DoS) flaw was found in the way the TLS/SSL protocol defined processing of ALERT packets during a connection handshake. A remote attacker could use this flaw to make a TLS/SSL server consume an excessive amount of CPU and fail to accept connections form other clients. Accordingly, the following vulnerabilities are addressed in this document that may affect the TLS/SSL data-plane of ACOS devices.

Item #	Vulnerability ID	Score Source	Score	Summary
1	CVE-2016-8610	RedHat	Medium	SSL/TLS: Malformed plain-text ALERT packets could cause remote DoS [1, 2, 3]

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
4.1.1			4.1.1-P1
4.1.0	–	4.1.0-P7	4.1.0-P8
2.7.2	–	2.7.2-P9	2.7.2-P10
2.7.1-GR1	–	2.7.1-GR1-P2	2.7.1-GR1-P3
2.6.1-GR1	–	2.6.1-GR1-P16	2.7.1-GR1-P3, 2.7.2-P10, 4.1.0-P8, 4.1.1-P1

WORKAROUNDS AND MITIGATIONS

Exposure to this vulnerability can be mitigated by configuring firewalls to limit the number of connections per IP address, or use deep packet inspection to reject this type of alert packets.

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-2016-8610	A flaw was found in the way OpenSSL processed ALERT packets during an SSL handshake. A attacker basically sends a large number of plaintext WARNING pkgs after CLIENTHELLO, which causes OpenSSL to go into a endless loop (while the attacker keeps on sending more alert packets), consequently taking 100% CPU. This may cause certain applications compiled against OpenSSL to hang and may not be able to serve content to the clients. This is specifically true about for servers which do not for or allocate extra thread for the processing of ClientHello like nginx.

RELATED LINKS

Ref #	General Link
[1]	NIST NVD, CVE-2016-8610
[2]	Red Hat, Inc - CVE-2016-8610
[3]	Bug 1384743 - (CVE-2016-8610) CVE-2016-8610 SSL/TLS: Malformed plain-text ALERT packets could cause remote DoS

ACKNOWLEDGEMENTS

None

MODIFICATION HISTORY

Revision	Date	Description
1.0	2017-07-25	Initial Publication

© Copyright 2017 A10 Networks, Inc. All Rights Reserved.

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.