TLS-SSL- CVE-2022-4450

PUBLISHED: APRIL 28, 2023 | LAST UPDATE: APRIL 28, 2023

Summary

On November 1, 2022, OpenSSL disclosed [1] OpenSSL vulnerabilities including CVE-2022-4450. This vulnerability affects the ACOS SSL/TLS Data Plane and is addressed in this document.

Item #	Vulnerability ID	Score Source	Score	Summary
1	CVE-2022-4304	CVSSv3	5.9 Medium	openssl: double free after calling PEM_read_bio_ex [2]

Affected Releases

The table below indicates releases of ACOS exposed to this vulnerability 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
5.0.0	–	5.2.1-P6	5.2.1-P7

Workarounds and Mitigations

None

Software Updates

Software updates that address these vulnerabilities are or will be published at the following URL:

https://support.a10networks.com/

©2023 A10 Networks, Inc. All rights reserved.

Vulnerability Details

The following table shares brief descriptions for the vulnerabilities addressed in this document.

Vulnerability ID	Description
CVE-2022-4450	The function PEM_read_bio_ex() reads a PEM file from a BIO and parses and decodes the "name" (e.g. "CERTIFICATE"), any header data and the payload data. If the function succeeds then the "name_out", "header" and "data" arguments are populated with pointers to buffers containing the relevant decoded data. The caller is responsible for freeing those buffers. It is possible to construct a PEM file that results in 0 bytes of payload data. In this case PEM_read_bio_ex() will return a failure code but will populate the header argument with a pointer to a buffer that has already been freed. If the caller also frees this buffer then a double free will occur. This will most likely lead to a crash. This could be exploited by an attacker who has the ability to supply malicious PEM files for parsing to achieve a denial of service attack. The functions PEM_read_bio() and PEM_read() are simple wrappers around PEM_read_bio_ex() and therefore these functions are also directly affected. These functions are also called indirectly by a number of other OpenSSL functions including PEM_X509_INFO_read_bio_ex() and SSL_CTX_use_serverinfo_file() which are also vulnerable. Some OpenSSL internal uses of these functions are not vulnerable because the caller does not free the header argument if PEM_read_bio_ex() returns a failure code. These locations include the PEM_read_bio_TYPE() functions as well as the decoders introduced in OpenSSL 3.0. The OpenSSL asn1parse command line application is also impacted by this issue.

Related Links

Ref #	General Link
[1]	https://www.openssl.org/news/secadv/20230207.txt
[2]	http://nvd.nist.gov/vuln/detail/CVE-2022-4450

Acknowledgements

None

Modification History

Revision	Date	Description
1.0	2023-4-28	Initial Publication

© Copyright 2023 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.