TLS-SSL- CVE-2022-4304

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

Summary

On November 1, 2022, OpenSSL disclosed [1] OpenSSL vulnerabilities including CVE-2022-4304 involving A timing based side channel exists in the OpenSSL RSA Decryption implementation which could be sufficient to recover a plaintext across a network in a Bleichenbacher style attack. This vulnerability affects the ACOS SSL/TLS Data Plane and Management Plane and is addressed in this document.

Item #	Vulnerability ID	Score Source	Score	Summary
1	CVE-2022-4304	CVSSv3	5.9 Medium	openssl: timing attack in RSA Decryption implementation [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 for Data Plane
5.0.0	–	5.2.1	None [a] for Management Plane
4.1.4-GR1			5.2.1-P7 for Data Plane
4.1.4-GR1			None [a] for Management Plane

(a) A10 continues to plan remediation for 5.2.1 and 4.1.4-GR1 Management Plane, pending availability of integrated corrections from upstream operating system providers.

Workarounds and Mitigations

This issue is valid for the 4.1.4 Data Plane Software SSL. 4.1.4 Hardware SSL is not affected.

To mitigate this issue, A10 recommends upgrading to 5.2.1-P7 and use swssl-tls13 mode.

Software Updates

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

https://support.a10networks.com/

Vulnerability Details

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

Vulnerability ID	Description
CVE-2022-4304	A timing based side channel exists in the OpenSSL RSA Decryption implementation which could be sufficient to recover a plaintext across a network in a Bleichenbacher style attack. To achieve a successful decryption an attacker would have to be able to send a very large number of trial messages for decryption. The vulnerability affects all RSA padding modes: PKCS#1 v1.5, RSA-OEAP and RSASVE. For example, in a TLS connection, RSA is commonly used by a client to send an encrypted pre-master secret to the server. An attacker that had observed a genuine connection between a client and a server could use this flaw to send trial messages to the server and record the time taken to process them. After a sufficiently large number of messages the attacker could recover the pre-master secret used for the original connection and thus be able to decrypt the application data sent over that connection.

Related Links

Ref #	General Link
[1]	https://www.openssl.org/news/secadv/20230207.txt
[2]	http://nvd.nist.gov/vuln/detail/CVE-2022-4304

Acknowledgements

None

Modification History

Revision	Date	Description
1.0	2023-4-28	Initial Publication

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.