ZLIB- CVE-2018-25032

PUBLISHED: MAY 12, 2022 | LAST UPDATE: MAY 26, 2022

Summary

In March 2022, a vulnerability in the “zlib” data compression library [1] was published [2]. The vulnerability, addressed in this document, could impact operations when restoring configuration information in ACOS systems that enable L3V (Layer 3 Virtualization) partitions and features.

Item #	Vulnerability ID	Score Source	Score	Summary
1	CVE-2018-25032	CVSSv3	1.9 Low [a]	zlib: A flaw in zlib-1.2.11 when compressing (not decompressing!) certain inputs. [3]

[a] CVSS score vector indicated with vulnerability details below.

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-P4	5.2.1-P5
4.1.4-GR1	–	4.1.4-GR1-P10	4.1.4-GR1-P11

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/

Vulnerability Details

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

Vulnerability ID	Description
CVE-2018-25032	zlib before 1.2.12 allows memory corruption when deflating (i.e., when compressing) if the input has many distant matches. (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)

Related Links

Ref #	General Link
[1]	zlib Data Compression Library - github
[2]	CVE-2018-25032 (zlib memory corruption on deflate) #605
[3]	NIST NVD, CVE-2018-25032

Acknowledgements

None

Modification History

Revision	Date	Description
1.0	2022-05-12	Initial Publication
1.1	2022-05-26	Updated CVE-2018-25032 scoring to 1.9 Low

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.