EXPAT- 2022 CVES- GROUP 1

PUBLISHED: AUGUST 26, 2022 | LAST UPDATE: SEPTEMBER 29, 2022

Summary

In January - February 2022, a number of vulnerabilities were disclosed [1,2,3] for the expat (libexpat) library where a remote attacker providing specially crafted XML content could potential result in Denial-of-Service (DoS) impacts or arbitrary code execution on ACOS systems. These vulnerabilities are addressed in this document. They may affect ACOS management plane services, including external health monitors processing XML content, and data plane services involving the use of aFlex to parse XML content. ACOS aFlex commands are not themselves exposed to this vulnerability.

Item		**Score**		
#	**Vulnerability ID**	**Source**	**Score**	**Summary**
0	CVE-2021-45960	CVSSv3	8.8 High	expat: Large number of prefixed XML attributes on a single tag can crash libexpat [4]
1	CVE-2021-46143	CVSSv3	7.8 High	expat: Integer overflow in doProlog in xmlparse.c [5]
2	CVE-2022-22822	CVSSv3	9.8 Critical	expat: Integer overflow in addBinding in xmlparse.c [6]
3	CVE-2022-22823	CVSSv3	9.8 Critical	expat: Integer overflow in build_model in xmlparse.c [7]
4	CVE-2022-22824	CVSSv3	9.8 Critical	expat: Integer overflow in defineAttribute in xmlparse.c [8]
5	CVE-2022-22825	CVSSv3	8.8 High	expat: Integer overflow in lookup in xmlparse.c [9]
6	CVE-2022-22826	CVSSv3	8.8 High	expat: Integer overflow in nextScaffoldPart in xmlparse.c [10]
7	CVE-2022-22827	CVSSv3	8.8 High	expat: Integer overflow in storeAtts in xmlparse.c [11]
8	CVE-2022-23852	CVSSv3	9.8 Critical	expat: Integer overflow in function XML_GetBuffer [12]
9	CVE-2022-25235	CVSSv3	9.8 Critical	expat: Malformed 2- and 3-byte UTF-8 sequences can lead to arbitrary code execution [13]
10	CVE-2022-25236	CVSSv3	9.8 Critical	expat: Namespace-separator characters in "xmlns[:prefix]" attribute values can lead to arbitrary code execution [14]
11	CVE-2022-25315	CVSSv3	9.8 Critical	expat: Integer overflow in storeRawNames() [15]

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-P5	5.2.1-P6
5.0.1 TPS	–	5.0.2-P1-TPS	5.0.2-P2-TPS
4.1.4-GR1	–	4.1.4-GR1-P10	4.1.4-GR1-P11
3.2.3-P1	–	3.2.5-P6	5.0.2-P2 TPS

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-2021-45960	In Expat (aka libexpat) before 2.4.3, a left shift by 29 (or more) places in the storeAtts function in xmlparse.c can lead to realloc misbehavior (e.g., allocating too few bytes, or only freeing memory).
CVE-2021-46143	In doProlog in xmlparse.c in Expat (aka libexpat) before 2.4.3, an integer overflow exists for m_groupSize.
CVE-2022-22822	addBinding in xmlparse.c in Expat (aka libexpat) before 2.4.3 has an integer overflow.
CVE-2022-22823	build_model in xmlparse.c in Expat (aka libexpat) before 2.4.3 has an integer overflow.
CVE-2022-22824	defineAttribute in xmlparse.c in Expat (aka libexpat) before 2.4.3 has an integer overflow.
CVE-2022-22825	lookup in xmlparse.c in Expat (aka libexpat) before 2.4.3 has an integer overflow.
CVE-2022-22826	nextScaffoldPart in xmlparse.c in Expat (aka libexpat) before 2.4.3 has an integer overflow.
CVE-2022-22827	storeAtts in xmlparse.c in Expat (aka libexpat) before 2.4.3 has an integer overflow.
CVE-2022-23852	Expat (aka libexpat) before 2.4.4 has a signed integer overflow in XML_GetBuffer, for configurations with a nonzero XML_CONTEXT_BYTES.
CVE-2022-25235	xmltok_impl.c in Expat (aka libexpat) before 2.4.5 lacks certain validation of encoding, such as checks for whether a UTF-8 character is valid in a certain context.
CVE-2022-25236	xmlparse.c in Expat (aka libexpat) before 2.4.5 allows attackers to insert namespace-separator characters into namespace URIs.
CVE-2022-25315	In Expat (aka libexpat) before 2.4.5, there is an integer overflow in storeRawNames.

Related Links

Ref #	General Link
[1]	Expat, Release 2.4.3 Changes
[2]	Expat, Release 2.4.4 Changes
[3]	Expat, Release 2.4.5 Changes
[4]	NIST NVD, CVE-2021-45960
[5]	NIST NVD, CVE-2021-46143
[6]	NIST NVD, CVE-2022-22822
[7]	NIST NVD, CVE-2022-22823
[8]	NIST NVD, CVE-2022-22824
[9]	NIST NVD, CVE-2022-22825
[10]	NIST NVD, CVE-2022-22826
[11]	NIST NVD, CVE-2022-22827
[12]	NIST NVD, CVE-2022-23852
[13]	NIST NVD, CVE-2022-25235
[14]	NIST NVD, CVE-2022-25236
[15]	NIST NVD, CVE-2022-25315

Acknowledgements

None

Modification History

Revision	Date	Description
1.0	2022-08-26	Initial Publication
2.0	2022-09-29	Indicated that aFlex commands are not affected. Refine exposure to parsing of XML content.

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.