WAF/SSLI – XML VULNERABILITIES

PUBLISHED: NOVEMBER 27, 2018 | LAST UPDATE: NOVEMBER 27, 2018

SUMMARY

Several vulnerabilities have been resolved in ACOS that could potentially affect Web Application Firewall (WAF) and SSL Insight (SSLi) services. Accordingly, the following vulnerabilities are addressed in this document.

Item #	Vulnerability ID	Score Source	Score	Summary
1	CVE-2016-4449	cvss3.0	7.1 High	libxml2: Inappropriate fetch of entities content
2	CVE-2016-4448	cvss3.0	9.8 Crit	libxml2: Format string vulnerability
3	CVE-2016-4447	cvss3.0	7.5 High	libxml2: Heap-based buffer underreads due to xmlParseName
4	CVE-2016-3705	cvss3.0	7.5 High	libxml2: stack overflow before detecting invalid XML file
5	CVE-2016-3627	cvss3.0	7.5 High	libxml2: stack exhaustion while parsing xml files in recovery mode
6	CVE-2016-2073	cvss3.0	6.5 Med	libxml2: out-of-bounds read in htmlParseNameComplex()
7	CVE-2016-1840	cvss3.0	8.8 High	libxml2: Heap-buffer-overflow in xmlFAParserPosCharGroup
8	CVE-2016-1839	cvss3.0	8.8 High	libxml2: Heap-based buffer overread in xmlDictAddString
9	CVE-2016-1838	cvss3.0	8.8 High	libxml2: Heap-based buffer overread in xmlPArserPrintFileContextInternal
10	CVE-2016-1837	cvss3.0	8.8 High	libxml2: Heap use-after-free in htmlPArsePubidLiteral and htmlParseSystemiteral
11	CVE-2016-1836	cvss3.0	8.8 High	libxml2: Heap use-after-free in xmlDictComputeFastKey
12	CVE-2016-1835	cvss3.0	8.8 High	libxml2: Heap use-after-free in xmlSAX2AttributeNs
13	CVE-2016-1834	cvss3.0	8.8 High	libxml2: Heap-buffer-overflow in xmlStrncat
14	CVE-2016-1833	cvss3.0	8.8 High	libxml2: Heap-based buffer overread in htmlCurrentChar
15	CVE-2016-1762	cvss3.0	9.8 Crit	libxml2: Heap-based buffer-overread in xmlNextChar
16	CVE-2015-8806	cvss3.0	7.5 High	libxml2: heap-buffer overread in dict.c
17	CVE-2015-8710	cvss3.0	9.8 Crit	libxml2: out-of-bounds memory access when parsing an unclosed HTML comment
18	CVE-2015-8317	cvss 2.0	5.0 Med	libxml2: Out-of-bounds heap read when parsing file with unfinished xml declaration
19	CVE-2015-8242	cvss 2.0	5.8 Med	libxml2: Buffer overread with HTML parser in push mode in xmlSAX2TextNode
20	CVE-2015-8241	cvss 2.0	6.4 Med	libxml2: Buffer overread with XML parser in xmlNextChar
21	CVE-2015-7942	cvss 2.0	6.8 Med	libxml2: heap-based buffer overflow in xmlParseConditionalSections()
22	CVE-2015-7941	cvss 2.0	4.3 Med	libxml2: Out-of-bounds memory access
23	CVE-2015-7500	cvss 2.0	5.0 Med	libxml2: Heap buffer overflow in xmlParseMisc
24	CVE-2015-7499	cvss 2.0	5.0 Med	libxml2: Heap-based buffer overflow in xmlGROW
25	CVE-2015-7498	cvss 2.0	5.0 Med	libxml2: Heap-based buffer overflow in xmlParseXmlDecl
26	CVE-2015-7497	cvss 2.0	5.0 Med	libxml2: Heap-based buffer overflow in xmlDictComputeFastQKey
27	CVE-2015-5312	cvss 2.0	7.1 High	libxml2: CPU exhaustion when processing specially crafted XML input
28	CVE-2015-1819	cvss 2.0	5.0 Med	libxml2: denial of service processing a crafted XML document
29	CVE-2014-3660	cvss 2.0	5.0 Med	libxml2: denial of service via recursive entity expansion
30	CVE-2014-0191	cvss 2.0	4.3 Med	libxml2: external parameter entity loaded when entity substitution is disabled
31	CVE-2013-1969	cvss 2.0	7.5 High	libxml2: multiple use-after-free flaws

32	CVE-2013-0339	cvss 2.0	6.8 Med	libxml2: CPU consumption DoS and other effects when performing string substitutions during external entities expansion
33	CVE-2013-0338	cvss 2.0	4.3 Med	libxml2: CPU consumption DoS when performing string substitutions during entities expansion
34	CVE-2012-5134	cvss 2.0	6.8 Med	libxml2: Heap-buffer-underflow in xmlParseAttValueComplex
35	A10-2018-0008 [(a)]	A10	High	libxml2: ACOS 2.7.x, 4.1.0/1/2, 4.1.4 vulnerabilities

[(a)] A10 Networks, Inc. assigned identifier.

AFFECTED RELEASES

The table below indicates releases of ACOS exposed to these vulnerabilities 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
4.1.4	–	4.1.4-P2	4.1.4-P3
4.1.2	–	4.1.2-P4	4.1.2-P5
4.1.1	–	4.1.1-P9	4.1.1-P10
4.1.0	–	4.1.0-P11	4.1.0-P12
2.7.2	–	2.7.2-Px	4.1.0-P12, 4.1.1-P10, 4.1.4-P3
2.7.1-GR1	–	2.7.1-GR1-Px	4.1.0-P12, 4.1.1-P10, 4.1.4-P3

WORKAROUNDS AND MITIGATIONS

In lieu of upgrading to a resolved release indicated above and recognizing the potential impact on functionality provided by the ACOS system, the following mitigations are available.

To mitigate WAF exposures, disable ACOS WAF processing and support for XML content by configuring WAF templates with configuration commands.

```
no xml-format-check
no xml-limit
no xml-sqlia-check
no xml-validation
no xml-xss-check
no soap-format-check
```

To mitigate SSLi exposures, disable ACOS SSLi processing and support for XML content by configuring SSLi templates with configuration commands.

```
no type xmpp
```

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-2016-4449	XML external entity (XXE) vulnerability in the xmlStringLenDecodeEntities function in parser.c in libxml2 before 2.9.4, when not in validating mode, allows context-dependent attackers to read arbitrary files or cause a denial of service (resource consumption) via unspecified vectors.
CVE-2016-4448	Format string vulnerability in libxml2 before 2.9.4 allows attackers to have unspecified impact via format string specifiers in unknown vectors.
CVE-2016-4447	The xmlParseElementDecl function in parser.c in libxml2 before 2.9.4 allows context-dependent attackers to cause a denial of service (heap-based buffer underread and application crash) via a crafted file, involving xmlParseName.
CVE-2016-3705	The (1) xmlParserEntityCheck and (2) xmlParseAttValueComplex functions in parser.c in libxml2 2.9.3 do not properly keep track of the recursion depth, which allows context-dependent attackers to cause a denial of service (stack consumption and application crash) via a crafted XML document containing a large number of nested entity references.
CVE-2016-3627	The xmlStringGetNodeList function in tree.c in libxml2 2.9.3 and earlier, when used in recovery mode, allows context-dependent attackers to cause a denial of service (infinite recursion, stack consumption, and application crash) via a crafted XML document.
CVE-2016-2073	The htmlParseNameComplex function in HTMLparser.c in libxml2 allows attackers to cause a denial of service (out-of-bounds read) via a crafted XML document.
CVE-2016-1840	Heap-based buffer overflow in the xmlFAParsePosCharGroup function in libxml2 before 2.9.4, as used in Apple iOS before 9.3.2, OS X before 10.11.5, tvOS before 9.2.1, and watchOS before 2.2.1, allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted XML document.
CVE-2016-1839	The xmlDictAddString function in libxml2 before 2.9.4, as used in Apple iOS before 9.3.2, OS X before 10.11.5, tvOS before 9.2.1, and watchOS before 2.2.1, allows remote attackers to cause a denial of service (heap-based buffer over-read) via a crafted XML document.
CVE-2016-1838	The xmlPArserPrintFileContextInternal function in libxml2 before 2.9.4, as used in Apple iOS before 9.3.2, OS X before 10.11.5, tvOS before 9.2.1, and watchOS before 2.2.1, allows remote attackers to cause a denial of service (heap-based buffer over-read) via a crafted XML document.
CVE-2016-1837	Multiple use-after-free vulnerabilities in the (1) htmlPArsePubidLiteral and (2) htmlParseSystemiteral functions in libxml2 before 2.9.4, as used in Apple iOS before 9.3.2, OS X before 10.11.5, tvOS before 9.2.1, and watchOS before 2.2.1, allow remote attackers to cause a denial of service via a crafted XML document.
CVE-2016-1836	Use-after-free vulnerability in the xmlDictComputeFastKey function in libxml2 before 2.9.4, as used in Apple iOS before 9.3.2, OS X before 10.11.5, tvOS before 9.2.1, and watchOS before 2.2.1, allows remote attackers to cause a denial of service via a crafted XML document.
CVE-2016-1835	Use-after-free vulnerability in the xmlSAX2AttributeNs function in libxml2 before 2.9.4, as used in Apple iOS before 9.3.2 and OS X before 10.11.5, allows remote attackers to cause a denial of service via a crafted XML document.
CVE-2016-1834	Heap-based buffer overflow in the xmlStrncat function in libxml2 before 2.9.4, as used in Apple iOS before 9.3.2, OS X before 10.11.5, tvOS before 9.2.1, and watchOS before 2.2.1, allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted XML document.
CVE-2016-1833	The htmlCurrentChar function in libxml2 before 2.9.4, as used in Apple iOS before 9.3.2, OS X before 10.11.5, tvOS before 9.2.1, and watchOS before 2.2.1, allows remote attackers to cause a denial of service (heap-based buffer over-read) via a crafted XML document.
CVE-2016-1762	The xmlNextChar function in libxml2 before 2.9.4 allows remote attackers to cause a denial of service (heap-based buffer over-read) via a crafted XML document.

CVE-2015-8806	dict.c in libxml2 allows remote attackers to cause a denial of service (heap-based buffer over-read and application crash) via an unexpected character immediately after the "<!DOCTYPE html" substring in a crafted HTML document.
CVE-2015-8710	The htmlParseComment function in HTMLparser.c in libxml2 allows attackers to obtain sensitive information, cause a denial of service (out-of-bounds heap memory access and application crash), or possibly have unspecified other impact via an unclosed HTML comment.
CVE-2015-8317	The xmlParseXMLDecl function in parser.c in libxml2 before 2.9.3 allows context-dependent attackers to obtain sensitive information via an (1) unterminated encoding value or (2) incomplete XML declaration in XML data, which triggers an out-of-bounds heap read.
CVE-2015-8242	The xmlSAX2TextNode function in SAX2.c in the push interface in the HTML parser in libxml2 before 2.9.3 allows context-dependent attackers to cause a denial of service (stack-based buffer over-read and application crash) or obtain sensitive information via crafted XML data.
CVE-2015-8241	The xmlNextChar function in libxml2 2.9.2 does not properly check the state, which allows context-dependent attackers to cause a denial of service (heap-based buffer over-read and application crash) or obtain sensitive information via crafted XML data.
CVE-2015-7942	The xmlParseConditionalSections function in parser.c in libxml2 does not properly skip intermediary entities when it stops parsing invalid input, which allows context-dependent attackers to cause a denial of service (out-of-bounds read and crash) via crafted XML data, a different vulnerability than CVE-2015-7941.
CVE-2015-7941	libxml2 2.9.2 does not properly stop parsing invalid input, which allows context-dependent attackers to cause a denial of service (out-of-bounds read and libxml2 crash) via crafted XML data to the (1) xmlParseEntityDecl or (2) xmlParseConditionalSections function in parser.c, as demonstrated by non-terminated entities.
CVE-2015-7500	The xmlParseMisc function in parser.c in libxml2 before 2.9.3 allows context-dependent attackers to cause a denial of service (out-of-bounds heap read) via unspecified vectors related to incorrect entities boundaries and start tags.
CVE-2015-7499	Heap-based buffer overflow in the xmlGROW function in parser.c in libxml2 before 2.9.3 allows context-dependent attackers to obtain sensitive process memory information via unspecified vectors.
CVE-2015-7498	Heap-based buffer overflow in the xmlParseXmlDecl function in parser.c in libxml2 before 2.9.3 allows context-dependent attackers to cause a denial of service via unspecified vectors related to extracting errors after an encoding conversion failure.
CVE-2015-7497	Heap-based buffer overflow in the xmlDictComputeFastQKey function in dict.c in libxml2 before 2.9.3 allows context-dependent attackers to cause a denial of service via unspecified vectors.
CVE-2015-5312	The xmlStringLenDecodeEntities function in parser.c in libxml2 before 2.9.3 does not properly prevent entity expansion, which allows context-dependent attackers to cause a denial of service (CPU consumption) via crafted XML data, a different vulnerability than CVE-2014-3660.
CVE-2015-1819	The xmlreader in libxml allows remote attackers to cause a denial of service (memory consumption) via crafted XML data, related to an XML Entity Expansion (XEE) attack.
CVE-2014-3660	parser.c in libxml2 before 2.9.2 does not properly prevent entity expansion even when entity substitution has been disabled, which allows context-dependent attackers to cause a denial of service (CPU consumption) via a crafted XML document containing a large number of nested entity references, a variant of the "billion laughs" attack.
CVE-2014-0191	The xmlParserHandlePEReference function in parser.c in libxml2 before 2.9.2, as used in Web Listener in Oracle HTTP Server in Oracle Fusion Middleware 11.1.1.7.0, 12.1.2.0, and 12.1.3.0 and other products, loads external parameter entities regardless of whether entity substitution or validation is enabled, which allows remote attackers to cause a denial of service (resource consumption) via a crafted XML document.
CVE-2013-1969	Multiple use-after-free vulnerabilities in libxml2 2.9.0 and possibly other versions might allow context-dependent attackers to cause a denial of service (crash) and possibly execute arbitrary code via vectors related to the (1) htmlParseChunk and (2) xmldecl_done functions, as demonstrated by a buffer overflow in the xmlBufGetInputBase function.

CVE-2013-0339	libxml2 through 2.9.1 does not properly handle external entities expansion unless an application developer uses the xmlSAX2ResolveEntity or xmlSetExternalEntityLoader function, which allows remote attackers to cause a denial of service (resource consumption), send HTTP requests to intranet servers, or read arbitrary files via a crafted XML document, aka an XML External Entity (XXE) issue. NOTE: it could be argued that because libxml2 already provides the ability to disable external entity expansion, the responsibility for resolving this issue lies with application developers; according to this argument, this entry should be REJECTed and each affected application would need its own CVE.
CVE-2013-0338	libxml2 2.9.0 and earlier allows context-dependent attackers to cause a denial of service (CPU and memory consumption) via an XML file containing an entity declaration with long replacement text and many references to this entity, aka "internal entity expansion" with linear complexity.
CVE-2012-5134	Heap-based buffer underflow in the xmlParseAttValueComplex function in parser.c in libxml2 2.9.0 and earlier, as used in Google Chrome before 23.0.1271.91 and other products, allows remote attackers to cause a denial of service or possibly execute arbitrary code via crafted entities in an XML document.
A10-2017-0008	libxml2 – dated library update/upgrade

RELATED LINKS

Ref #	General Link
[1]	http://nvd.nist.gov/vuln/detail/CVE-2016-4449
[2]	http://nvd.nist.gov/vuln/detail/CVE-2016-4448
[3]	http://nvd.nist.gov/vuln/detail/CVE-2016-4447
[4]	http://nvd.nist.gov/vuln/detail/CVE-2016-3705
[5]	http://nvd.nist.gov/vuln/detail/CVE-2016-3627
[6]	http://nvd.nist.gov/vuln/detail/CVE-2016-2073
[7]	http://nvd.nist.gov/vuln/detail/CVE-2016-1840
[8]	http://nvd.nist.gov/vuln/detail/CVE-2016-1839
[9]	http://nvd.nist.gov/vuln/detail/CVE-2016-1838
[10]	http://nvd.nist.gov/vuln/detail/CVE-2016-1837
[11]	http://nvd.nist.gov/vuln/detail/CVE-2016-1836
[12]	http://nvd.nist.gov/vuln/detail/CVE-2016-1835
[13]	http://nvd.nist.gov/vuln/detail/CVE-2016-1834
[14]	http://nvd.nist.gov/vuln/detail/CVE-2016-1833
[15]	http://nvd.nist.gov/vuln/detail/CVE-2016-1762
[16]	http://nvd.nist.gov/vuln/detail/CVE-2015-8806
[17]	http://nvd.nist.gov/vuln/detail/CVE-2015-8710
[18]	http://nvd.nist.gov/vuln/detail/CVE-2015-8317
[19]	http://nvd.nist.gov/vuln/detail/CVE-2015-8242
[20]	http://nvd.nist.gov/vuln/detail/CVE-2015-8241
[21]	http://nvd.nist.gov/vuln/detail/CVE-2015-7942
[22]	http://nvd.nist.gov/vuln/detail/CVE-2015-7941
[23]	http://nvd.nist.gov/vuln/detail/CVE-2015-7500
[24]	http://nvd.nist.gov/vuln/detail/CVE-2015-7499
[25]	http://nvd.nist.gov/vuln/detail/CVE-2015-7498
[26]	http://nvd.nist.gov/vuln/detail/CVE-2015-7497
[27]	http://nvd.nist.gov/vuln/detail/CVE-2015-5312
[28]	http://nvd.nist.gov/vuln/detail/CVE-2015-1819
[29]	http://nvd.nist.gov/vuln/detail/CVE-2014-3660
[30]	http://nvd.nist.gov/vuln/detail/CVE-2014-0191
[31]	http://nvd.nist.gov/vuln/detail/CVE-2013-1969
[32]	http://nvd.nist.gov/vuln/detail/CVE-2013-0339
[33]	http://nvd.nist.gov/vuln/detail/CVE-2013-0338
[34]	http://nvd.nist.gov/vuln/detail/CVE-2012-5134

ACKNOWLEDGEMENTS

None

MODIFICATION HISTORY

Revision	Date	Description
1.0	2018-11-27	Initial Publication