SYSTEM - VULNERABILITIES #1 - ACOS 3.X, 4.X

PUBLISHED: AUGUST 7, 2017 | LAST UPDATE: OCTOBER 11, 2019

SUMMARY

A number of vulnerabilities have surfaced in the Operating System (OS) supported in ACOS 3.x and 4.x. Accordingly, the following vulnerabilities are addressed in this document.

Item #	Vulnerability ID	Score Source	Score	Summary
1	CVE-2015-2059	CVSS 2.0	7.5 High	libidn: out-of-bounds read with stringprep on invalid UTF-8. [1]
2	CVE-2011-1425	CVSS 2.0	7.5 High	xmlsec1: arbitrary file creation when verifying signatures [2]
3	CVE-2015-7696	CVSS 3.0	6.8 Med	unzip: Heap overflow and DoS in 6.0 [3]
4	CVE-2014-9471	CVSS 2.0	7.5 High	coreutils: memory corruption flaw in parse_datetime() [4]
5	CVE-2016-4008	CVSS 3.0	5.9 Med	libtasn1: infinite loop while parsing DER certificates [5]
6	CVE-2015-2806	CVSS 2.0	10.0 High	libtasn1: stack overflow in asn1_der_decoding [6]
7	CVE-2015-1782	CVSS 2.0	6.8 Med	libssh2: Using SSH_MSG_KEXINIT data unbounded [7]
8	CVE-2013-2154	CVSS 2.0	7.5 High	xml-security-c: Stack-based buffer overflow when evaluating certain XPointer expressions [8]
9	CVE-2013-2156	CVSS 2.0	7.5 High	xml-security-c: Heap-based buffer overflow when processing certain PrefixList attribute values in the Exclusive Canonicalization mode [9]
10	CVE-2013-2210	CVSS 2.0	7.5 High	xml-security-c: Heap-buffer overflow during XPointer evaluation [10]
11	CVE-2014-8121	CVSS 2.0	5.0 Med	glibc: Unexpected closing of nss_files databases after lookups causes denial of service [11]
12	CVE-2017-7308	CVSS 3.0	7.8 High	kernel: net/packet: overflow in check for priv area size [12]
13	CVE-2017-7294	CVSS 3.0	7.8 High	kernel: drm/vmwgfx: fix integer overflow in vmw_surface_define_ioctl() [13]
14	CVE-2017-7187	CVSS 3.0	7.8 High	kernel: scsi: Stack-based buffer overflow in sg_ioctl function [14]
15	CVE-2017-7184	CVSS 3.0	7.8 High	kernel: Out-of-bounds heap access in xfrm [15]
16	CVE-2017-2636	CVSS 3.0	7.8 High	kernel: Race condition access to n_hdlc.tbuf causes double free in n_hdlc_release() [16]
17	CVE-2016-10200	CVSS 3.0	7.0 High	kernel: l2tp: Race condition in the L2TPv3 IP encapsulation feature [17]
18	CVE-2017-5972	CVSS 3.0	7.5High	kernel: SYN cookie protection mechanism not properly implemented [18]

AFFECTED RELEASES

The table below indicates releases of ACOS exposed to these vulnerabilities and ACOS releases that address these issues or are otherwise unaffected by them.

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
4.1.2	–	4.1.2-P1	4.1.2-P2
4.1.1	–	4.1.1-P3	4.1.1-P4
4.1.100	–	4.1.100-P5	4.1.100-P5-SP1 [a], 4.1.100-P6 [b]
4.1.0	–	4.1.0-P9	4.1.0-P10 [a], 4.1.0-P11 [b]
3.1.0-P1	–	3.2.1-P1	3.2.2-P1

[a] Addresses items 1 – 11 listed above.

[b] Additionally addresses items 12 – 18 listed above.

WORKAROUNDS AND MITIGATIONS

Common security best practices in the industry for network appliance management and control planes can enhance protection against remote malicious attacks. Limit the exploitable attack surface for critical, infrastructure, networking equipment through the use of access lists or firewall filters to and from only trusted, administrative networks or hosts.

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-2015-2059	The stringprep_utf8_to_ucs4 function in libin before 1.31, as used in jabberd2, allows context-dependent attackers to read system memory and possibly have other unspecified impact via invalid UTF-8 characters in a string, which triggers an out-of-bounds read.
CVE-2011-1425	xslt.c in XML Security Library (aka xmlsec) before 1.2.17, as used in WebKit and other products, when XSLT is enabled, allows remote attackers to create or overwrite arbitrary files via vectors involving the libxslt output extension and a ds:Transform element during signature verification.
CVE-2015-7696	Info-ZIP UnZip 6.0 allows remote attackers to cause a denial of service (heap-based buffer over-read and application crash) or possibly execute arbitrary code via a crafted password-protected ZIP archive, possibly related to an Extra-Field size value.
CVE-2014-9471	The parse_datetime function in GNU coreutils allows remote attackers to cause a denial of service (crash) or possibly execute arbitrary code via a crafted date string, as demonstrated by the "--date=TZ="123"345" @1" string to the touch or date command.
CVE-2016-4008	The _asn1_extract_der_octet function in lib/decoding.c in GNU Libtasn1 before 4.8, when used without the ASN1_DECODE_FLAG_STRICT_DER flag, allows remote attackers to cause a denial of service (infinite recursion) via a crafted certificate.
CVE-2015-2806	Stack-based buffer overflow in asn1_der_decoding in libtasn1 before 4.4 allows remote attackers to have unspecified impact via unknown vectors.
CVE-2015-1782	The kex_agree_methods function in libssh2 before 1.5.0 allows remote servers to cause a denial of service (crash) or have other unspecified impact via crafted length values in an SSH_MSG_KEXINIT packet.
CVE-2013-2154	Stack-based buffer overflow in the XML Signature Reference functionality (xsec/dsig/DSIGReference.cpp) in Apache Santuario XML Security for C++ (aka xml-security-c) before 1.7.1 allows context-dependent attackers to cause a denial of service (crash) and possibly execute arbitrary code via malformed XPointer expressions, probably related to the DSIGReference::getURIBaseTXFM function.
CVE-2013-2156	Heap-based buffer overflow in the Exclusive Canonicalization functionality (xsec/canon/XSECC14n20010315.cpp) in Apache Santuario XML Security for C++ (aka xml-security-c) before 1.7.1 allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via a crafted PrefixList attribute.
CVE-2013-2210	Heap-based buffer overflow in the XML Signature Reference functionality in Apache Santuario XML Security for C++ (aka xml-security-c) before 1.7.2 allows context-dependent attackers to cause a denial of service (crash) and possibly execute arbitrary code via malformed XPointer expressions. NOTE: this is due to an incorrect fix for CVE-2013-2154.

CVE-2014-8121	DB_LOOKUP in nss_files/files-XXX.c in the Name Service Switch (NSS) in GNU C Library (aka glibc or libc6) 2.21 and earlier does not properly check if a file is open, which allows remote attackers to cause a denial of service (infinite loop) by performing a look-up on a database while iterating over it, which triggers the file pointer to be reset.
CVE-2017-7308	The packet_set_ring function in net/packet/af_packet.c in the Linux kernel through 4.10.6 does not properly validate certain block-size data, which allows local users to cause a denial of service (integer signedness error and out-of-bounds write), or gain privileges (if the CAP_NET_RAW capability is held), via crafted system calls.
CVE-2017-7294	The vmw_surface_define_ioctl function in drivers/gpu/drm/vmwgfx/vmwgfx_surface.c in the Linux kernel through 4.10.6 does not validate addition of certain levels data, which allows local users to trigger an integer overflow and out-of-bounds write, and cause a denial of service (system hang or crash) or possibly gain privileges, via a crafted ioctl call for a /dev/dri/renderD* device.
CVE-2017-7187	The sg_ioctl function in drivers/scsi/sg.c in the Linux kernel through 4.10.4 allows local users to cause a denial of service (stack-based buffer overflow) or possibly have unspecified other impact via a large command size in an SG_NEXT_CMD_LEN ioctl call, leading to out-of-bounds write access in the sg_write function.
CVE-2017-7184	The xfrm_replay_verify_len function in net/xfrm/xfrm_user.c in the Linux kernel through 4.10.6 does not validate certain size data after an XFRM_MSG_NEWAE update, which allows local users to obtain root privileges or cause a denial of service (heap-based out-of-bounds access) by leveraging the CAP_NET_ADMIN capability, as demonstrated during a Pwn2Own competition at CanSecWest 2017 for the Ubuntu 16.10 linux-image-* package 4.8.0.41.52.
CVE-2017-2636	Race condition in drivers/tty/n_hdlc.c in the Linux kernel through 4.10.1 allows local users to gain privileges or cause a denial of service (double free) by setting the HDLC line discipline.
CVE-2016-10200	Race condition in the L2TPv3 IP Encapsulation feature in the Linux kernel before 4.8.14 allows local users to gain privileges or cause a denial of service (use-after-free) by making multiple bind system calls without properly ascertaining whether a socket has the SOCK_ZAPPED status, related to net/l2tp/l2tp_ip.c and net/l2tp/l2tp_ip6.c.
CVE-2017-5972	The TCP stack in the Linux kernel 3.x does not properly implement a SYN cookie protection mechanism for the case of a fast network connection, which allows remote attackers to cause a denial of service (CPU consumption) by sending many TCP SYN packets, as demonstrated by an attack against the kernel-3.10.0 package in CentOS Linux 7. NOTE: third parties have been unable to discern any relationship between the GitHub Engineering finding and the Trigemini.c attack code.

RELATED LINKS

Ref #	General Link
[1]	NIST NVD, CVE-2015-2059
[2]	NIST NVD, CVE-2011-1425
[3]	NIST NVD, CVE-2015-7696
[4]	NIST NVD, CVE-2014-9471
[5]	NIST NVD, CVE-2016-4008
[6]	NIST NVD, CVE-2015-2806
[7]	NIST NVD, CVE-2015-1782
[8]	NIST NVD, CVE-2013-2154
[9]	NIST NVD, CVE-2013-2156
[10]	NIST NVD, CVE-2013-2210
[11]	NIST NVD, CVE-2014-8121
[12]	NIST NVD, CVE-2017-7308
[13]	NIST NVD, CVE-2017-7294
[14]	NIST NVD, CVE-2017-7187
[15]	NIST NVD, CVE-2017-7184
[16]	NIST NVD, CVE-2017-2636
[17]	NIST NVD, CVE-2016-10200
[18]	NIST NVD, CVE-2017-5972

ACKNOWLEDGEMENTS

None

MODIFICATION HISTORY

Revision	Date	Description
1.0	2017-08-07	Initial Publication
2.0	2018-03-07	Update release information for ACOS 4.1.0.
3.0	2019-10-11	Added 4.1.100 release family.