SYSTEM - VULNERABILITIES #2 - ACOS 3.X, 4.X

PUBLISHED: SEPTEMBER 12, 2018 | 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-2018-1111	CVSS 3.0	7.5 High	DHCP Command injection vulnerability in the DHCP client NetworkManager integration script [1]
2	CVE-2016-1000110	Red Hat	5.0 Med	Python CGIHandler: sets environmental variable based on user supplied Proxy request header [2]
3	CVE-2016-5699	CVSS 3.0	6.1 Med	python: http protocol steam injection attack [3]
4	CVE-2016-5636	CVSS 3.0	9.8 Critical	python: Heap overflow in zipimporter module [4]
5	CVE-2016-0772	CVSS 3.0	4.8 Med	python: smtplib StartTLS stripping attack [5]

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
4.1.4	–	4.1.4-P1	4.1.4-P2
4.1.2	–	4.1.2-P4	4.1.2-P5
4.1.1	–	4.1.1-P8	4.1.1-P9
4.1.100	–	4.1.100-P5	4.1.100-P5-SP1
4.1.0	–	4.1.0-P11	4.1.0-P12
3.1.0-P1	–	3.2.2-P5	3.2.2-P6, 3.2.3

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-2018-1111	DHCP packages in Red Hat Enterprise Linux 6 and 7, Fedora 28, and earlier are vulnerable to a command injection flaw in the NetworkManager integration script included in the DHCP client. A malicious DHCP server, or an attacker on the local network able to spoof DHCP responses, could use this flaw to execute arbitrary commands with root privileges on systems using NetworkManager and configured to obtain network configuration using the DHCP protocol.
CVE-2016-1000110	It was discovered that the Python CGIHandler class did not properly protect against the HTTP_PROXY variable name clash in a CGI context. A remote attacker could possibly use this flaw to redirect HTTP requests performed by a Python CGI script to an attacker-controlled proxy via a malicious HTTP request.
CVE-2016-5699	It was found that the Python's httplib library (used by urllib, urllib2 and others) did not properly check HTTPConnection.putheader() function arguments. An attacker could use this flaw to inject additional headers in a Python application that allowed user provided header names or values.
CVE-2016-5636	A vulnerability was discovered in Python, in the built-in zipimporter. A specially crafted zip file placed in a module path such that it would be loaded by a later "import" statement could cause a heap overflow, leading to arbitrary code execution.
CVE-2016-0772	It was found that Python's smtplib library did not return an exception when StartTLS failed to be established in the SMTP.starttls() function. A man in the middle attacker could strip out the STARTTLS command without generating an exception on the Python SMTP client application, preventing the establishment of the TLS layer.

RELATED LINKS

Ref #	General Link
[1]	NIST NVD, CVE-2018-1111
[2]	NIST NVD, CVE-2016-1000110
[3]	NIST NVD, CVE-2016-5699
[4]	NIST NVD, CVE-2016-5636
[5]	NIST NVD, CVE-2016-0772

ACKNOWLEDGEMENTS

None

MODIFICATION HISTORY

Revision	Date	Description
1.0	2018-09-12	Initial Publication
2.0	2019-10-11	Added 4.1.100 release family.