Alpine Linux - Bug #9565

Bug # 9563 (Closed): libxml2: Multiple vulnerabilities (CVE-2018-9251, CVE-2018-14404, CVE-2018-14567)

[3.8] libxml2: Multiple vulnerabilities (CVE-2018-9251, CVE-2018-14404, CVE-2018-14567)

10/23/2018 10:59 AM - Alicha CH

Status:	Closed	**Start date:**	10/23/2018
Priority:	Normal	**Due date:**	
Assignee:	Carlo Landmeter	**% Done:**	100%
Category:	Security	**Estimated time:**	0.00 hour
Target version:	3.8.2		
Affected versions:		**Security IDs:**	

Description

CVE-2018-9251: The xz_decomp function in xzlib.c in libxml2 2.9.8, if --with-lzma is used, allows remote attackers to cause a denial of service (infinite loop) via
a crafted XML file that triggers LZMA_MEMLIMIT_ERROR, as demonstrated by xmllint, a different vulnerability than CVE-2015-8035.

References:

https://bugzilla.gnome.org/show_bug.cgi?id=794914

Patch:

https://gitlab.gnome.org/GNOME/libxml2/commit/2240fbf5912054af025fb6e01e26375100275e74

CVE-2018-14404: A NULL pointer dereference vulnerability exists in the xpath.c:xmlXPathCompOpEval() function of libxml2 through 2.9.8 when parsing an invalid XPath expression in the XPATH_OP_AND or XPATH_OP_OR case. Applications processing untrusted XSL format inputs with the use of the libxml2 library may be vulnerable to a denial of service attack due to a crash of the application.

References:

https://gitlab.gnome.org/GNOME/libxml2/issues/5
https://people.canonical.com/~ubuntu-security/cve/2018/CVE-2018-14404.html

Patch:

https://gitlab.gnome.org/GNOME/libxml2/commit/a436374994c47b12d5de1b8b1d191a098fa23594

CVE-2018-14567: libxml2 2.9.8, if --with-lzma is used, allows remote attackers to cause a denial of service (infinite loop) via a crafted XML file that triggers
LZMA_MEMLIMIT_ERROR, as demonstrated by xmllint, a different vulnerability than CVE-2015-8035 and CVE-2018-9251.

References:

https://gitlab.gnome.org/GNOME/libxml2/issues/13
https://people.canonical.com/~ubuntu-security/cve/2018/CVE-2018-14567.html

Patch:

https://gitlab.gnome.org/GNOME/libxml2/commit/2240fbf5912054af025fb6e01e26375100275e74

Associated revisions

Revision 9ba0323a - 10/24/2018 04:20 PM - Natanael Copa

main/libxml2: backport security fixes

- CVE-2018-9251
- CVE-2018-14404
- CVE-2018-14567

fixes #9565

History

#1 - 10/24/2018 04:23 PM - Natanael Copa

- Status changed from New to Resolved

- % Done changed from 0 to 100

Applied in changeset alpine:9ba0323ae03ecb1319c9174e281260c37544fa1d.

#2 - 10/25/2018 07:05 AM - Alicha CH

- Project changed from Alpine Security to Alpine Linux

- Category set to Security

- Status changed from Resolved to Closed

- Security IDs deleted (CVE-2018-9251, CVE-2018-14404, CVE-2018-14567)