Alpine Linux - Bug #9897

Bug # 9895 (Resolved): libraw: Multiple vulnerabilities (CVE-2018-20363, CVE-2018-20364, CVE-2018-20365, CVE-2018-5817 CVE-2018-5818, CVE-2018-5819)

[3.8] libraw: Multiple vulnerabilities (CVE-2018-20363, CVE-2018-20364, CVE-2018-20365, CVE-2018-5817 CVE-2018-5818, CVE-2018-5819)

01/23/2019 04:33 PM - Alicha CH

Status:	Rejected	**Start date:**	01/23/2019
Priority:	Normal	**Due date:**	
Assignee:	Natanael Copa	**% Done:**	0%
Category:		**Estimated time:**	0.00 hour
Target version:	3.8.2		
Affected versions:		**Security IDs:**	CVE-2018-20363, CVE-2018-20364, CVE-2018-20365, CVE-2018-5817 CVE-2018-5818, CVE-2018-5819

Description

CVE-2018-20363: LibRaw::raw2image in libraw_cxx.cpp in LibRaw 0.19.1 has a NULL pointer dereference.

References:

https://github.com/LibRaw/LibRaw/issues/193

Patches:

Fixed by: https://github.com/LibRaw/LibRaw/commit/7e29b9f29449fde30cc878fbb137d61c14bba3a4
Additionally needed: https://github.com/LibRaw/LibRaw/commit/a7c17cb6bbec1e79f058d84511f9c3b142cbdfa7

CVE-2018-20364: LibRaw::copy_bayer in libraw_cxx.cpp in LibRaw 0.19.1 has a NULL pointer dereference.

References:

https://github.com/LibRaw/LibRaw/issues/194
https://nvd.nist.gov/vuln/detail/CVE-2018-20364

Patches:

Fixed by: https://github.com/LibRaw/LibRaw/commit/7e29b9f29449fde30cc878fbb137d61c14bba3a4
Additionally needed: https://github.com/LibRaw/LibRaw/commit/a7c17cb6bbec1e79f058d84511f9c3b142cbdfa7

CVE-2018-20365: LibRaw::raw2image() in libraw_cxx.cpp has a heap-based buffer overflow.

References:

https://github.com/LibRaw/LibRaw/issues/195
https://nvd.nist.gov/vuln/detail/CVE-2018-20365

Patches:

Fixed by: https://github.com/LibRaw/LibRaw/commit/7e29b9f29449fde30cc878fbb137d61c14bba3a4
Additionally needed: https://github.com/LibRaw/LibRaw/commit/a7c17cb6bbec1e79f058d84511f9c3b142cbdfa7

CVE-2018-5817: DoS in unpacked_load_raw function in internal/dcraw_common.cpp

Fixed In Version:

LibRaw 0.19.1

References:

https://www.flexera.com/company/secunia-research/advisories/SR-2018-27.html

Patch:

https://github.com/LibRaw/LibRaw/commit/e67a9862d10ebaa97712f532eca1eb5e2e410a22

CVE-2018-5818:DoS in parse_rollei function in internal/dcraw_common.cpp

Fixed In Version:

0.19.1

References:

https://www.flexera.com/company/secunia-research/advisories/SR-2018-27.html

Patch:

https://github.com/LibRaw/LibRaw/commit/e67a9862d10ebaa97712f532eca1eb5e2e410a22

CVE-2018-5819: DoS in parse_sinar_ia function in internal/dcraw_common.cpp

Fixed In Version:

0.19.1

References:

https://www.flexera.com/company/secunia-research/advisories/SR-2018-27.html

Patch:

https://github.com/LibRaw/LibRaw/commit/e67a9862d10ebaa97712f532eca1eb5e2e410a22

History

#1 - 01/31/2019 02:51 PM - Leonardo Arena

- Status changed from New to Rejected

Won't fix. Requires 0.19.x