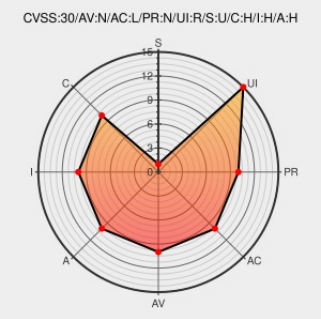
CVE-2018-5809

Published on: 12/07/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:45 PM UTC

CVE-2018-5809

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Libraw from Libraw contain the following vulnerability:

An error within the "LibRaw::parse_exif()" function (internal/dcraw_common.cpp) in LibRaw versions prior to 0.18.9 can be exploited to cause a stack-based buffer overflow and subsequently execute arbitrary code.

CVE-2018-5809 has been assigned by PSIRT-CNA@flexerasoftware.com to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 8.8 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	REQUIRED
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: 6.8 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
LibRaw/Changelog.txt at master · LibRaw/LibRaw · GitHub	Release Notes, github.com, text/html	MISC github.com/LibRaw/LibRaw/blob/master/Changelog.txt

Secunia 81800#1: samsumg_load_raw · LibRaw/LibRaw@fd63302 · GitHub	Patch github.com text/html	MISC github.com/LibRaw/LibRaw/commit/fd6330292501983ac75fe4162275794b18
Computer Security Research - Secunia	Third Party Advisory secuniaresearch.flexerasoftware.com text/html	MISC secuniaresearch.flexerasoftware.com/secunia_research/2018-9/
Security Advisory SA81800 - LibRaw Multiple Vulnerabilities - Secunia	Third Party Advisory secuniaresearch.flexerasoftware.com text/html	SECUNIA 81800

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Libraw	Libraw	All	All	All	All
Application	Libraw	Libraw	All	All	All	All

cpe:2.3:a:libraw:libraw:*:*:*:*:*:*:*:*:

cpe:2.3:a:libraw:libraw:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→