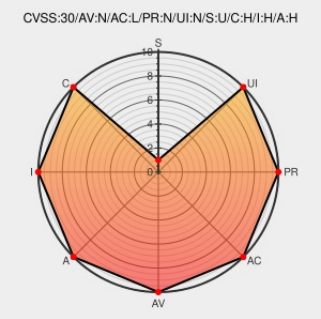
CVE-2017-6890

Published on: 05/15/2017 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:50 PM UTC

CVE-2017-6890

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



Certain versions of Libraw-demosaic-pack-gpl2 from Libraw contain the following vulnerability:

A boundary error within the "foveon_load_camf()" function (dcraw_foveon.c) when initializing a huffman table in LibRaw-demosaic-pack-GPL2 before 0.18.2 can be exploited to cause a stack-based buffer overflow.

CVE-2017-6890 has been assigned by PSIRT-CNA@flexerasoftware.com to track the vulnerability - currently rated as CRITICAL severity.

Affected Vendor/Software: **LibRaw** - **LibRaw-demosaic-pack-GPL2** version **0.x prior to 0.18.2**

CVSS3 Score: 9.8 - CRITICAL

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

CVSS2 Score: 7.5 - HIGH

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

CVE References

Description	Tags	Link
End of Support for the Secunia Community Site - Community	Permissions Required Third Party Advisory	MISC secuniaresearch.flexerasoftware.com/advisories/75000/

	secuniaresearch.flexerasoftware.com text/html	
Fixed possible foveon buffer overrun (Secunia SA750000) · LibRaw/LibRaw-demosaic-pack-GPL2@194f592 · GitHub	Patch Third Party Advisory github.com text/html	CONFIRM github.com/LibRaw/LibRaw-demosaic-pack-GPL2/commit/194f592e205990ea8fce72b6c571c14350aca716

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-demosaic-pack-gpl2	All	All	All	All

cpe:2.3:a:libraw:libraw-demosaic-pack-gpl2:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→