



CVE-2020-35535

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

Summary

CVE	CVE-2020-35535
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-09-01 18:15:00 UTC
Updated	2022-09-07 17:33:00 UTC
Description	In LibRaw, there is an out-of-bounds read vulnerability within the "LibRaw::parseSonySRF()" function (libraw/src/metadata&

Risk And Classification

Problem Types: CWE-125

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Libraw	Libraw	0.20.0	-	All	All
Application	Libraw	Libraw	0.20.0	rc2	All	All
Application	Libraw	Libraw	0.20.1	All	All	All
Application	Libraw	Libraw	0.20.2	All	All	All
Application	Libraw	Libraw	0.21.0	beta1	All	All

References

Reference	Source	Link	Ta
Libraw "LibRaw::parseSonySRF()" Out-of-bounds Read Vulnerability · Issue #283 · LibRaw/LibRaw · GitHub	MISC	github.com	
additional checks in parseSonySRF · LibRaw/LibRaw@c243f45 · GitHub	MISC	github.com	
CVE Program record	CVE.ORG	www.cve.org	ca
NVD vulnerability detail	NVD	nvd.nist.gov	ca

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[502878](#) Alpine Linux Security Update for libraw

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)