CVE-2018-20096

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2018-20096
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-12-12 10:29:00 UTC
Updated	2023-11-07 02:56:00 UTC
Description	There is a heap-based buffer over-read in the Exiv2::tEXtToDataBuf function of pngimage.cpp in Exiv2 0.27-RC3. A crafted

Risk And Classification

Problem Types: CWE-125

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Exiv2	Exiv2	0.27	rc3	All	All
Application	Exiv2	Exiv2	0.27	rc3	All	All

References

Reference	Source	Link
[SECURITY] Fedora 30 Update: mingw-exiv2-0.27-3.fc30 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org
pocs/exiv2/20181206 at master · TeamSeri0us/pocs · GitHub	MISC	github.com
[SECURITY] Fedora 30 Update: mingw-exiv2-0.27-3.fc30 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org
Several bugs in exiv2 0.27-rc3 · Issue #590 · Exiv2/exiv2 · GitHub	MISC	github.com
Red Hat Customer Portal	REDHAT	access.redhat.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

377485 Alibaba Cloud Linux Security Update for exiv2 (ALINUX2-SA-2019:0103)

671123 EulerOS Security Update for exiv2 (EulerOS-SA-2019-2144)

940399 AlmaLinux Security Update for exiv2 (ALSA-2020:1577)

960313 Rocky Linux Security Update for exiv2 (RLSA-2020:1577)