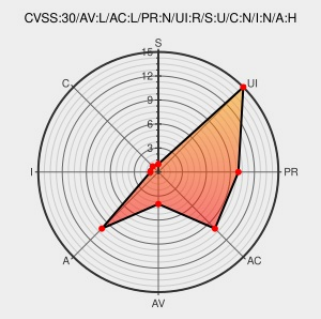
CVE-2017-14866

Published on: 09/28/2017 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:45 PM UTC

CVE-2017-14866

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



Certain versions of Exiv2 from Exiv2 contain the following vulnerability:

There is a heap-based buffer overflow in the Exiv2::s2Data function of types.cpp in Exiv2 0.26. A Crafted input will lead to a denial of service attack.

CVE-2017-14866 has been assigned by cve@mitre.org to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 5.5 - MEDIUM

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

CVSS2 Score: 4.3 - MEDIUM

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

CVE References

Description	Tags	Link
1494781 – It is a heap-buffer-overflow in Exiv2::s2Data (types.cpp:383)	Exploit Issue Tracking Third Party Advisory bugzilla.redhat.com text/html	MISC bugzilla.redhat.com/show_bug.cgi?id=1494781

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Exiv2	Exiv2	0.26	All	All	All
Application	Exiv2	Exiv2	0.26	All	All	All

cpe:2.3:a:exiv2:exiv2:0.26:*:*:*:*:*:*:*:

cpe:2.3:a:exiv2:exiv2:0.26:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→