

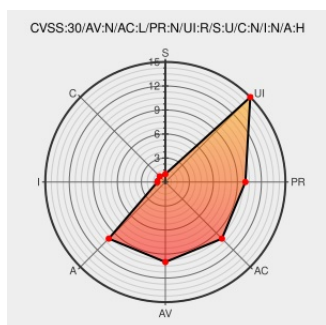


CVE-2018-20537

Published on: 12/27/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:36 PM UTC

CVE-2018-20537

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Liblas](#) from [Liblas](#) contain the following vulnerability:

There is a NULL pointer dereference at `liblas::SpatialReference::GetGTIF()` (`spatialreference.cpp`) in `libLAS` 1.8.1 that will cause a denial of service.

CVE-2018-20537 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **6.5 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	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
[SECURITY] Fedora 31 Update: liblas-1.8.1-5.fc31 - package-announce - Fedora Mailing-Lists	lists.fedoraproject.org text/html	FEDORA FEDORA-2020-b0695cdf7
[SECURITY] Fedora 32 Update: liblas-1.8.1-5.fc32 - package-announce - Fedora Mailing-Lists	lists.fedoraproject.org text/html	FEDORA FEDORA-2020-6dbbecb893

1652611 – There is an illegal address access at liblas::SpatialReference::GetGTIF()(src/spatialreference.cpp:532) in libLAS while will cause dos attack.

Exploit
Issue Tracking
Third Party Advisory
bugzilla.redhat.com
text/html

MISC
bugzilla.redhat.com/show_bug.cgi?id=1652611

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	Liblas	Liblas	1.8.1	All	All	All
Application	Liblas	Liblas	1.8.1	All	All	All
cpe:2.3:a:liblas:liblas:1.8.1:****:****:						
cpe:2.3:a:liblas:liblas:1.8.1:****:****:						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID→](#)