

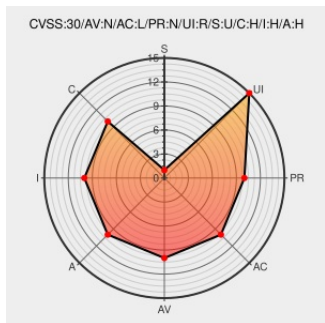


CVE-2018-20542

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

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

CVE-2018-20542

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

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

There is a heap-based buffer-overflow at `generator_spgemm_csc_reader.c` (function `libxsmm_sparse_csc_reader`) in LIBXSMM 1.10, a different vulnerability than CVE-2018-20541 (which is in a different part of the source code and is seen at a different address).

CVE-2018-20542 has been assigned by [M](#) [cve@mitre.org](#) to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **8.8 - HIGH**

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

CVSS2 Score: **6.8 - MEDIUM**

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

CVE References

Description	Tags	Link
Issue #287: made CSR/CSC readers more robust against invalid input (c... · hfp/libxsmm@1514814 · GitHub	Patch Third Party Advisory github.com	MISC github.com/hfp/libxsmm/commit/151481489192e6d1997f8bde52c5

text/html

reported buffer overflows · Issue #287 · hfp/libxsmm · GitHub

ExploitPatchThird Party Advisorygithub.comtext/html

MISC github.com/hfp/libxsmm/issues/287

1652633 – There is a heap-buffer-overflow at src/generator_spgemm_csc_reader.c:178(function libxsmm_sparse_csc_reader) that allocated at src/generator_spgemm_csc_reader.c:125 in libxsmm.

ExploitIssue TrackingThird Party Advisorybugzilla.redhat.comtext/html

MISC bugzilla.redhat.com/show_bug.cgi?id=1652633

1652635 – There is a heap-buffer-overflow that the heap is allocated at src/generator_spgemm_csc_reader.c:125 and triggered at function libxsmm_sparse_csc_reader in libxsmm.

ExploitIssue TrackingThird Party Advisorybugzilla.redhat.comtext/html

MISC bugzilla.redhat.com/show_bug.cgi?id=1652635

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	Libxsmm Project	Libxsmm	1.10	All	All	All
Application	Libxsmm Project	Libxsmm	1.10	All	All	All

cpe:2.3:a:libxsmm_project:libxsmm:1.10:*:*:*:*:*:

cpe:2.3:a:libxsmm_project:libxsmm:1.10:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID →