

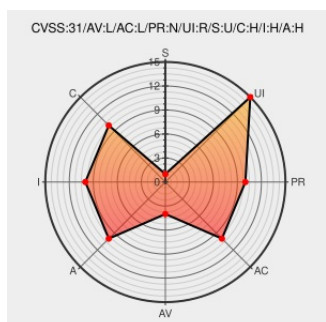


CVE-2020-11865

Published on: 05/11/2020 12:00:00 AM UTC

Last Modified on: 11/07/2023 03:15:00 AM UTC

CVE-2020-11865

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

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

libEMF (aka ECMA-234 Metafile Library) through 1.0.11 allows out-of-bounds memory access.

CVE-2020-11865 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **7.8 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	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
[security-announce] openSUSE-SU-2020:0831-1: important: Security update	lists.opensuse.org text/html	SUSE openSUSE-SU-2020:0831
ECMA-234 Metafile Library / News: Re-Release of libEMF-1.0.12	Patch Release Notes	MISC sourceforge.net/p/libemf/news/2020/05/re-

Third Party Advisory
sourceforge.net
text/html

release-of-libemf-1012/

ECMA-234 Metafile Library / List libemf-devel Archives

Third Party Advisory
sourceforge.net
text/html

MISC
sourceforge.net/p/libemf/mailman/libemf-devel/

[SECURITY] Fedora 31 Update: libEMF-1.0.12-1.fc31 - package-announce - Fedora Mailing-Lists

lists.fedoraproject.org
text/html

FEDORA FEDORA-2020-c696d8604b

ECMA-234 Metafile Library / Code / Browse Commits

Third Party Advisory
sourceforge.net
text/html

MISC
sourceforge.net/p/libemf/code/commit_browser

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
Operating System	Fedoraproject	Fedora	31	All	All	All
Operating System	Fedoraproject	Fedora	31	All	All	All
Application	Libemf Project	Libemf	All	All	All	All
Operating System	Opensuse	Leap	15.1	All	All	All
cpe:2.3:o:fedoraproject:fedora:31:*****:						
cpe:2.3:o:fedoraproject:fedora:31:*****:						
cpe:2.3:a:libemf_project:libemf:*****:						
cpe:2.3:o:opensuse:leap:15.1:*****:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @RemotelyAlerts	Severity: ?? libEMF (aka ECMA-234 Metafile Library) t... CVE-2020-11865 Link for more: alerts.remotelyrmm.com/CVE-2020-11865	2022-10-07 02:37:02

[← Previous ID](#)

[Next ID →](#)

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](#)