

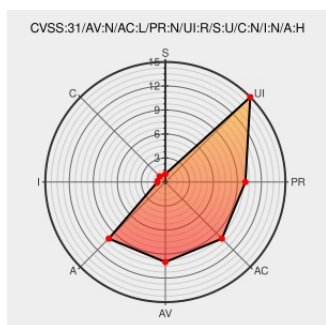


CVE-2019-16707

Published on: 09/23/2019 12:00:00 AM UTC

Last Modified on: 02/13/2023 07:08:00 PM UTC

CVE-2019-16707

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

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

Hunspell 1.7.0 has an invalid read operation in SuggestMgr::leftcommonsubstring in suggestmgr.cxx.

CVE-2019-16707 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: mingw-hunspell-1.7.0-6.fc31 - package-announce - Fedora Mailing-Lists	lists.fedoraproject.org text/html	FEDORA FEDORA-2019-074bf7d2d3
[SECURITY] Fedora 30 Update: hunspell-1.7.0-4.fc30 - package-announce - Fedora Mailing-Lists	lists.fedoraproject.org text/html	FEDORA FEDORA-2019-656f7ac8ca

[SECURITY] Fedora 30 Update: mingw-hunspell-1.7.0-6.fc30 - package-announce - Fedora Mailing-Lists

[lists.fedoraproject.org](https://lists.fedoraproject.org/text/html)
text/html

 FEDORA FEDORA-2019-746b0b02f7

[SECURITY] Fedora 31 Update: hunspell-1.7.0-4.fc31 - package-announce - Fedora Mailing-Lists

[lists.fedoraproject.org](https://lists.fedoraproject.org/text/html)
text/html

 FEDORA FEDORA-2019-7841e28c1b

GitHub - butterflyhack/hunspell-crash: find a crash by libfuzzer

[Exploit](#)
[Third Party Advisory](#)
github.com
text/html

 MISC
github.com/butterflyhack/hunspell-crash

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.

Related QID Numbers

[377493](#) Alibaba Cloud Linux Security Update for hunspell (ALINUX2-SA-2020:0142)

[500252](#) Alpine Linux Security Update for hunspell

[670182](#) EulerOS Security Update for hunspell (EulerOS-SA-2021-1680)

[670279](#) EulerOS Security Update for hunspell (EulerOS-SA-2021-1798)

[670624](#) EulerOS Security Update for hunspell (EulerOS-SA-2021-2382)

[901481](#) Common Base Linux Mariner (CBL-Mariner) Security Update for hunspell (7244)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Fedoraproject	Fedora	30	All	All	All
Operating System	Fedoraproject	Fedora	31	All	All	All
Application	Hunspell Project	Hunspell	1.7.0	All	All	All
Application	Hunspell Project	Hunspell	1.7.0	All	All	All
cpe:2.3:o:fedoraproject:fedora:30:*:*:*:*:*:						
cpe:2.3:o:fedoraproject:fedora:31:*:*:*:*:*:						
cpe:2.3:a:hunspell_project:hunspell:1.7.0:*:*:*:*:*:						
cpe:2.3:a:hunspell_project:hunspell:1.7.0:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

[← 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](#)