



CVE-2018-12932

Published on: 06/28/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:22 PM UTC

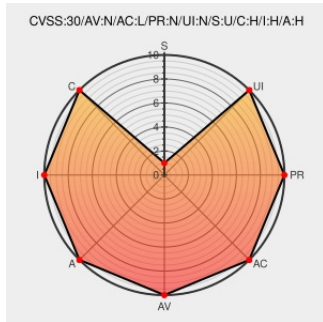
CVE-2018-12932

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



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

PlayEnhMetaFileRecord in enhmetafile.c in Wine 3.7 allows attackers to cause a denial of service (heap-based buffer overflow) or possibly have unspecified other impact by triggering a large pAlphaBlend->cbBitsSrc value.

CVE-2018-12932 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **CRITICAL** severity.

CVSS3 Score: **9.8 - CRITICAL**

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

CVSS2 Score: **7.5 - HIGH**

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

CVE References

Description	Tags	Link
	Issue Tracking Patch Third Party Advisory bugs.winehq.org text/plain	MISC bugs.winehq.org/attachment.cgi?id=61284

Bug #1764719 "Security vulnerabilities in Wine when handling EMF..." : Bugs : wine package : Ubuntu

- Issue Tracking
- Third Party Advisory
- bugs.launchpad.net
- text/html

MISC bugs.launchpad.net/ubuntu/+source/wine/+bug/1764719

WineHQ Bugzilla – Bug 45105 – heap-buffer overflow in gdi32 (CVE-2018-12932)

- Issue Tracking
- Patch
- Third Party Advisory
- bugs.winehq.org
- text/html

MISC bugs.winehq.org/show_bug.cgi?id=45105

source.winehq.org Git - wine.git/commit

- Issue Tracking
- Patch
- Third Party Advisory
- source.winehq.org
- text/xml

MISC source.winehq.org/git/wine.git/commit/8d2676fd14f130f9e8f06744743423168bf8d18d

source.winehq.org Git - wine.git/commit

- Issue Tracking
- Patch
- Third Party Advisory
- source.winehq.org
- text/xml

MISC source.winehq.org/git/wine.git/commit/b6da3547d8990c3c3affc3a5865aefd2a0946949

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	Winehq	Wine	3.7	All	All	All
Application	Winehq	Wine	3.7	All	All	All

cpe:2.3:a:winehq:wine:3.7:*:*:*:*:*:

cpe:2.3:a:winehq:wine:3.7:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID →

© CVE.report 2023 |

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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status status.cve.report