



# CVE-2017-2905

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2017-2905
<b>State</b>	PUBLIC
<b>Assigner</b>	talos-cna@cisco.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2018-04-24 19:29:00 UTC
<b>Updated</b>	2022-06-13 19:07:00 UTC
<b>Description</b>	An exploitable integer overflow exists in the bmp loading functionality of the Blender open-source 3d creation suite version 2.78c. The overflow is triggered when loading a BMP file with a width of 0. This can be exploited to crash the application or, in some cases, to execute arbitrary code.

## Risk And Classification

**Problem Types:** CWE-190

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Blender</a>	<a href="#">Blender</a>	2.78c	All	All	All
Application	<a href="#">Blender</a>	<a href="#">Blender</a>	2.78c	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	8.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	9.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	8.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	9.0	All	All	All

## References

Reference	Source	Link	Tags
TALOS-2017-0412    Cisco Talos Intelligence Group - Comprehensive Threat Intelligence	MISC	<a href="http://www.talosintelligence.com">www.talosintelligence.com</a>	Exploit,
[SECURITY] [DLA 1465-1] blender security update	MLIST	<a href="http://lists.debian.org">lists.debian.org</a>	Mailing
Debian -- Security Information -- DSA-4248-1 blender	DEBIAN	<a href="http://www.debian.org">www.debian.org</a>	Third P
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>	canonic
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>	canonic

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

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](#)**