



CVE-2018-20185

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

Summary

CVE	CVE-2018-20185
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-12-17 19:29:00 UTC
Updated	2020-08-18 15:05:00 UTC
Description	In GraphicsMagick 1.4 snapshot-20181209 Q8 on 32-bit platforms, there is a heap-based buffer over-read in the ReadBMP

Risk And Classification

Problem Types: CWE-125

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Application	Graphicsmagick	Graphicsmagick	1.4	2018-12-09	All	All
Application	Graphicsmagick	Graphicsmagick	1.4	2018-12-09	All	All

References

Reference	Source	Link	Tags
USN-4207-1: GraphicsMagick vulnerabilities Ubuntu security notices	UBUNTU	usn.ubuntu.com	Third Party Advisor
[SECURITY] [DLA 1619-1] graphicsmagick security update	MLIST	lists.debian.org	Mailing List, Third Party
GraphicsMagick / Bugs / #582 heap-buffer-overflow in ReadBMPImage of bmp.c	MISC	sourceforge.net	Exploit, Third Party
GraphicsMagick: changeset 15864:648e3977a293	MISC	hg.graphicsmagick.org	Patch, Vendor Advisory

Malformed Request	BID	www.securityfocus.com	Third Party Advisor
Debian -- Security Information -- DSA-4640-1 graphicsmagick	DEBIAN	www.debian.org	Third Party Advisor
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

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