



CVE-2016-8685

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

Summary

CVE	CVE-2016-8685
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-01-31 22:59:00 UTC
Updated	2017-02-05 20:15:00 UTC
Description	The findnext function in decompose.c in potrace 1.13 allows remote attackers to cause a denial of service (invalid memory access) by sending a crafted image file.

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Potrace Project	Potrace	All	All	All	All

References

Reference	Source	Link	Tags
potrace: invalid memory access in findnext (decompose.c) agostino's blog	MISC	blogs.gentoo.org	Third Party Advisory
oss-security - Re: potrace: invalid memory access in findnext (decompose.c)	MLIST	www.openwall.com	Mailing List, Third Party Advisory
Potrace 'decompose.c' Memory Corruption Vulnerability	BID	www.securityfocus.com	Third Party Advisory, Vulnerability
oss-security - potrace: invalid memory access in findnext (decompose.c)	MLIST	www.openwall.com	Mailing List, Third Party Advisory
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.

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](#).

Free CVE JSON API cve.report/api

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