



CVE-2017-2575

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

Summary

CVE	CVE-2017-2575
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-08-22 21:29:00 UTC
Updated	2019-10-09 23:26:00 UTC
Description	A vulnerability was found while fuzzing libbpg 0.9.7. It is a NULL pointer dereference issue due to missing check of the return value of image_alloc().

Risk And Classification

Problem Types: CWE-476

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Libbpg Project	Libbpg	0.9.7	All	All	All
Application	Libbpg Project	Libbpg	0.9.7	All	All	All

References

Reference	Source	Link
libbpg 'image_alloc()' Function Null Pointer Dereference Denial of Service Vulnerability	BID	www.securityfocus.com/bid/79841
oss-sec: CVE-2017-2575 libbpg: NULL pointer dereference in image_alloc	MLIST	seclists.org/oss-sec/2017/08/22/cve-2017-2575
IBM X-Force Exchange	libbpg BPG encoder denial of service	exchange.xforce.ibmcloud.com/libbpg-BPG-encoder-denial-of-service
CVE Program record	CVE.ORG	www.cve.org/CVE.experts/CVE-2017-2575
NVD vulnerability detail	NVD	nvd.nist.gov/vuln/detail/CVE-2017-2575

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