



CVE-2017-7245

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2017-7245
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-03-23 21:59:00 UTC
Updated	2018-08-17 10:29:00 UTC
Description	Stack-based buffer overflow in the pcre32_copy_substring function in pcre_get.c in libpcre1 in PCRE 8.40 allows remote at

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Pcre	Pcre	8.40	All	All	All
Application	Pcre	Pcre	8.40	All	All	All

References

Reference	Source	Link
PCRE: Multiple vulnerabilities (GLSA 201710-25) — Gentoo Security	GENTOO	security.gentoo.org
libpcre Multiple Security Vulnerabilities	BID	www.securityfocus.com
libpcre: two stack-based buffer overflow write in pcre32_copy_substring (pcre_get.c) agostino's blog	MISC	blogs.gentoo.org
Red Hat Customer Portal	REDHAT	access.redhat.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[710566](#) Gentoo Linux PCRE Multiple Vulnerabilities (GLSA 201710-25)

[751361](#) SUSE Enterprise Linux Security Update for pcre (SUSE-SU-2021:3652-1)

© [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](#)