CVE-2017-7607

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2017-7607
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-04-09 14:59:00 UTC
Updated	2019-10-03 00:03:00 UTC
Description	The handle_gnu_hash function in readelf.c in elfutils 0.168 allows remote attackers to cause a denial of service (heap-base

Risk And Classification

Problem Types: CWE-125

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Elfutils Project	Elfutils	0.168	All	All	All
Application	Elfutils Project	Elfutils	0.168	All	All	All

References

Reference	Source	Link	Tags
[security-announce] openSUSE-SU-2019:1590-1: moderate: Security update f	SUSE	lists.opensuse.org	
elfutils: Multiple vulnerabilities (GLSA 201710-10) — Gentoo security	GENTOO	security.gentoo.org	
elfutils CVE-2017-7607 Remote Denial of Service Vulnerability	BID	www.securityfocus.com	
USN-3670-1: elfutils vulnerabilities | Ubuntu security notices | Ubuntu	UBUNTU	usn.ubuntu.com	
elfutils: heap-based buffer overflow in handle_gnu_hash (readelf.c) | agostino's blog	MISC	blogs.gentoo.org	Exploit, Patch, T
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analy

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

500172 Alpine Linux Security Update for elfutils

503908 Alpine Linux Security Update for elfutils

710326 Gentoo Linux elfutils Multiple Vulnerabilities (GLSA 201710-10)

752414 SUSE Enterprise Linux Security Update for dwarves and elfutils (SUSE-SU-2022:2614-1)

Free CVE JSON API cve.report/api

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