



CVE-2014-0172

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

Summary

CVE	CVE-2014-0172
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-04-11 15:55:00 UTC
Updated	2017-07-01 01:29:00 UTC
Description	Integer overflow in the check_section function in dwarf_begin_elf.c in the libdw library, as used in elfutils 0.153 and possibly

Risk And Classification

Problem Types: CWE-189

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Elfutils Project	Elfutils	0.153	All	All	All
Application	Elfutils Project	Elfutils	0.154	All	All	All
Application	Elfutils Project	Elfutils	0.155	All	All	All
Application	Elfutils Project	Elfutils	0.156	All	All	All
Application	Elfutils Project	Elfutils	0.157	All	All	All
Application	Elfutils Project	Elfutils	0.158	All	All	All
Application	Elfutils Project	Elfutils	0.153	All	All	All
Application	Elfutils Project	Elfutils	0.154	All	All	All
Application	Elfutils Project	Elfutils	0.155	All	All	All
Application	Elfutils Project	Elfutils	0.156	All	All	All
Application	Elfutils Project	Elfutils	0.157	All	All	All
Application	Elfutils Project	Elfutils	0.158	All	All	All

References

Reference	Source	Link
USN-2188-1: elfutils vulnerability Ubuntu	UBUNTU	www.ubuntu.com
Elfutils libdw 'check_section()' Function Remote Heap Based Buffer Overflow Vulnerability	BID	www.bidsa.org

1085663 – (CVE-2014-0172) CVE-2014-0172 elfutils: integer overflow, leading to a heap-based buffer overflow in libdw	CONFIRM	bugzilla
oss-sec: Heap-based buffer overflow in libdw/elfutils (CVE-2014-0172)	MLIST	seclist
[PATCH] CVE-2014-0172 Check for overflow before calling malloc to uncompress data.	MLIST	lists.fe
elfutils: Heap-based buffer overflow (GLSA 201612-32) — Gentoo security	GENTOO	securi
CVE Program record	CVE.ORG	www.c
NVD vulnerability detail	NVD	nvd.ni



No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.