



CVE-2017-16357

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

Summary

CVE	CVE-2017-16357
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-11-01 17:29:00 UTC
Updated	2017-11-13 16:27:00 UTC
Description	In radare 2.0.1, a memory corruption vulnerability exists in store_versioninfo_gnu_verdef() and store_versioninfo_gnu_vern

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Radare	Radare2	2.0.1	All	All	All
Application	Radare	Radare2	2.0.1	All	All	All

References

Reference	Source	Link	Tags
Fixed crash in elf.c with 32bit r2 when shdr->sh_size > max size_t · radareorg/radare2@0b973e2 · GitHub	CONFIRM	github.com	Issue
Memory corruption on 32bit system · Issue #8742 · radareorg/radare2 · GitHub	CONFIRM	github.com	Exploit
CVE Program record	CVE.ORG	www.cve.org	Canonical
NVD vulnerability detail	NVD	nvd.nist.gov	Canonical

No vendor comments have been submitted for this CVE.

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

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](#)