radare2 < 6.1.4 Command Injection via PDB Parser print_gvars()

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

Summary

CVE	CVE-2026-40499
State	PUBLISHED
Assigner	VulnCheck
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-15 04:17:48 UTC
Updated	2026-04-17 15:38:09 UTC
Description	radare2 prior to version 6.1.4 contains a command injection vulnerability in the PDB parser's print_gvars() function that allo

Risk And Classification

Primary CVSS: v4.0 8.4 HIGH from disclosure@vulncheck.com

CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:A/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

EPSS: 0.001240000 probability, percentile 0.315960000 (date 2026-04-17)

Problem Types: CWE-78 | CWE-78 CWE-78 Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')

Version	Source	Type	Score	Severity	Vector
4.0	disclosure@vulncheck.com	Secondary	8.4	HIGH	CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:A/VC:H/VI:H/VA:H/SC:N/SI:N/SA
4.0	CNA	CVSS	8.4	HIGH	CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:A/VC:H/VI:H/VA:H/SC:N/SI:N/SA

CVSS v4.0 Breakdown

Attack Vector

Local

Attack Complexity

Low

Attack Requirements

None

Privileges Required

None

User Interaction

Active

Active

Confidentiality

High

Integrity

High

Availability

High

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:A/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Radareorg	Radare2	affected 6.1.4 semver	Not specified
CNA	Radareorg	Radare2	unaffected 5590c87deeb7eb2a106fd7aab9ca88bfeebb7397 git	Not specified

References

Reference	Source	Link
github.com/radareorg/radare2/issues/25752	disclosure@vulncheck.com	github.com
github.com/radareorg/radare2/commit/5590c87deeb7eb2a106fd7aab9ca88bfeebb...	disclosure@vulncheck.com	github.com
www.vulncheck.com/advisories/radare2-command-injection-via-pdb-parser-print-gvars	disclosure@vulncheck.com	www.vulncheck.com
github.com/radareorg/radare2/releases/tag/6.1.4	disclosure@vulncheck.com	github.com
blog.calif.io/p/mad-bugs-discovering-a-0-day-in-zero	disclosure@vulncheck.com	blog.calif.io
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

Vendor Comments And Credit

Discovery Credit

CNA: junrong of Calif (en)

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