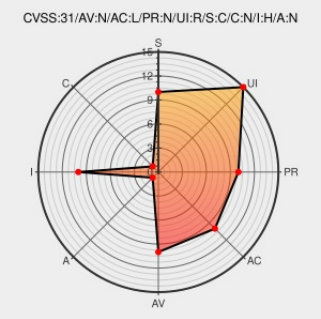
CVE-2020-15121

Published on: 07/20/2020 12:00:00 AM UTC

Last Modified on: 11/07/2023 03:17:00 AM UTC

CVE-2020-15121 - advisory for GHSA-r552-vp94-9358

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Fedora from Fedoraproject contain the following vulnerability:

In radare2 before version 4.5.0, malformed PDB file names in the PDB server path cause shell injection. To trigger the problem it's required to open the executable in radare2 and run idpd to trigger the download. The shell code will execute, and will create a file called pwned in the current directory.

CVE-2020-15121 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as CRITICAL severity.

Affected Vendor/Software: **radareorg** - **radare2** version **< 4.5.0**

CVSS3 Score: 9.6 - CRITICAL

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	REQUIRED
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
CHANGED	HIGH	HIGH	HIGH

CVSS2 Score: 6.8 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link

Command injection during opening PE file with malformed debug symbol information (PDB) - `idpd` command · Advisory · radareorg/radare2 · GitHub	Third Party Advisory github.com text/html	CONFIRM github.com/radareorg/radare2/security/advisories/GHSA-r552-vp94-9358
Command injection across r_sys_cmd* · Issue #16945 · radareorg/radare2 · GitHub	Third Party Advisory github.com text/html	MISC github.com/radareorg/radare2/issues/16945
Fix command injection on PDB download (#16966) · radareorg/radare2@04edfa8 · GitHub	Patch Third Party Advisory github.com text/html	MISC github.com/radareorg/radare2/commit/04edfa82c1f3fa2bc3621ccdad2f93bdbf00e4f9
Fix command injection on PDB download by GustavoLCR · Pull Request #16966 · radareorg/radare2 · GitHub	Third Party Advisory github.com text/html	MISC github.com/radareorg/radare2/pull/16966
[SECURITY] Fedora 32 Update: cutter-re-1.11.0-1.fc32 - package-announce - Fedora Mailing-Lists	lists.fedoraproject.org text/html	FEDORA FEDORA-2020-aa51efe207
[SECURITY] Fedora 31 Update: radare2-4.5.0-1.fc31 - package-announce - Fedora Mailing-Lists	lists.fedoraproject.org text/html	FEDORA FEDORA-2020-d5b33b6e6c

Related QID Numbers

501234 Alpine Linux Security Update for radare2

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Fedoraproject	Fedora	31	All	All	All
Operating System	Fedoraproject	Fedora	32	All	All	All
Application	Radare	Radare2	All	All	All	All
Application	Radare	Radare2	All	All	All	All

cpe:2.3:o:fedoraproject:fedora:31:*:*:*:*:*:*:*:

cpe:2.3:o:fedoraproject:fedora:32:*:*:*:*:*:*:*:

cpe:2.3:a:radare:radare2:*:*:*:*:*:*:*:*:

cpe:2.3:a:radare:radare2:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)

← Previous ID

Next ID→