Off-by-one Error in v2fly/v2ray-core

Valid Reported on Nov 7th 2021

0

Description

Good afternoon. While looking at your code, we discovered an `off-by-one index comparison against length may lead to out-of-bounds read` flaw in your v2ray-core repository. Indexing operations on arrays, slices or strings should use an index at most one less than the length. If the index to be accessed is checked for being less than or equal to the length (<=), instead of less than the length (<), the index could be out of bounds.

Proof of Concept

Please review lines 140-144 of `proxy/vmess/encoding/commands.go`, most specifically line 142.

```
cmd.Level = uint32(data[levelStart])
    timeStart := levelStart + 1
    if len(data) < timeStart {
        return nil, newError("insufficient length.")
    }
```

Impact

This vulnerability is capable of an out of bounds read.

Occurrences

commands.go L142

References

- CWE-193: Off-by-one Error

CVE
CVE-2021-4070
(Published)

Vulnerability Type
CWE-193: Off-by-one Error

Severity
Medium (5.9)

Visibility
Public

Status
Fixed

Found by

geeknik
@geeknik
unranked

This report was seen 501 times.

We are processing your report and will contact the v2fly/v2ray-core team within 24 hours. a year ago

We have contacted a member of the v2fly/v2ray-core team and are waiting to hear back a year ago

We have sent a follow up to the v2fly/v2ray-core team. We will try again in 7 days. a year ago

We have sent a second follow up to the v2fly/v2ray-core team. We will try again in 10 days. a year ago

We have sent a third and final follow up to the v2fly/v2ray-core team. This report is now considered stale. a year ago

A v2fly/v2ray-core maintainer a year ago Maintainer

Thanks for your report. This report is received by V2Fly Team, we are analyzing this report.
Shelikhoo

A v2fly/v2ray-core maintainer a year ago Maintainer

Thanks for your report and responsible disclosure.
I would like to say sorry for the slow response, it seems the mail from this platform went to the spam box...

The preliminary investigation on this shows that this vulnerability allows a VMess Server to crash a VMess Client by sending a specially crafted handshake response reply with an (optional) VMess SwitchAccount Command that is one byte shorter than expected.
Is this understanding of vulnerability correct?

We don't have a paid bounty program. This is not a substitution of monetary reward but, we would like to give you a special thanks in the release note when the fix is released. The credit will be given to this Github account: https://github.com/geeknik

geeknik a year ago Researcher

Yes, your root cause analysis is correct. The huntr.dev platform handles the bounty payments at no cost to your organization once you mark the issue as valid. Please. credit the posted GitHub account. Thank you.

A v2fly/v2ray-core maintainer validated this vulnerability a year ago

geeknik has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

A v2fly/v2ray-core maintainer a year ago Maintainer

We have issued an security update to fix this vulnerability.
The commit that fixed this vulnerability: https://github.com/v2fly/v2ray-core/commit/c1af2bfd7aa59a4482aa7f6ec4b9208c1d350b5c .
The security update release that includes this fix:
https://github.com/v2fly/v2ray-core/releases/tag/v4.44.0

Jamie Slome marked this as fixed in 4.44.0 with commit c1af2b 10 months ago

The fix bounty has been dropped ×

This vulnerability will not receive a CVE ×

commands.go#L142 has been validated ✓

Sign in to join this conversation