Reflected XSS in rtxteam/rtx

Valid Reported on Apr 29th 2022

0

Description

hello team, i found a reflected xss in `/rtxcomplete/nodeslike` via `callback` parameter

Proof of Concept

```
https://arax.rtx.ai/rtxcomplete/nodeslike?_=1651210002052&callback=%3CScRiP
```

Impact

Steal User Cookie or redirect to malicious sites

CVE
CVE-2022-1806
(Published)

Vulnerability Type
CWE-79: Cross-site Scripting (XSS) - Reflected

Severity
Medium (6.3)

Registry
Other

Affected Version
1.0

Visibility
Public

Status
Fixed

Found by

0xRaw

@0xraw

legend

This report was seen 720 times.

We are processing your report and will contact the **rtxteam/rtx** team within 24 hours. 7 months ago

We have contacted a member of the **rtxteam/rtx** team and are waiting to hear back 7 months ago

We have sent a follow up to the **rtxteam/rtx** team. We will try again in 7 days. 7 months ago

A **rtxteam/rtx** maintainer 7 months ago — Maintainer

Thank you, I am filing a bug report about this with our team.

0xRaw 7 months ago — Researcher

Thank you for the fast response highly appreciated.

We have sent a second follow up to the **rtxteam/rtx** team. We will try again in 10 days. 7 months ago

A **rtxteam/rtx** maintainer 7 months ago — Maintainer

Hi OxRaw, my team reports that they have figured out how to fix the issue and they are testing it out. Thank you for your patience. We will advise when the fix is committed to GitHub and deployed into production. We have opted not to track this in our public issue repository (but rather are tracking it in our private Slack workspace) since it is a security vulnerability in a public-facing system. Thanks again for reporting this to us. We will be in touch with an update within the next week.

A **rtxteam/rtx** maintainer validated this vulnerability 6 months ago

0xRaw has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

A **rtxteam/rtx** maintainer marked this as fixed in **checkpoint_2022-05-18** with commit **9bb109**
6 months ago

The fix bounty has been dropped ✖

This vulnerability will not receive a CVE ✖

0xRaw 6 months ago — Researcher

Hello thanks for the quick fix,
Can i have a CVE for this finding ?

Kind Regrads,
Rawi.

A **rtxteam/rtx** maintainer 6 months ago — Maintainer

Hi OxRaw, sure, can you please tell me how I can provide you the CVE? I am not so experienced with using the huntr.dev site. Thanks.

0xRaw 6 months ago — Researcher

Hey,
I'm not that expert too but from what i saw in previous reports that the user should request the CVE and the maintainer should reply with a yes or no based on the maintainer answer the CVE will be issued or not.
btw, I sent this report to an admin he will provide the CVE , since you agreed.

Kind Regards,
Rawi.

Jamie Slome 6 months ago — Admin

Sorted 👍

A **rtxteam/rtx** maintainer 6 months ago — Maintainer

Thank you Jamie.

Sign in to join this conversation