SQL injection vulnerability in ARAX-UI Synonym Lookup functionality in rtxteam/rtx

0

Valid Reported on Apr 15th 2022

Description

The `/rtxcomplete/nodeslike` endpoint in the ARAX-UI application at https://arax.rtx.ai is vulnerable to SQL injection. It is possible to include a malicious SQL payload in the `word` query parameter for this endpoint that would allow an attacker to dump the database, make modifications to data, or delete data. In addition it is possible to completely takeover the server where the application is hosted, by performing remote code execution via this vulnerability.

Proof of Concept

Perform a GET request to:

```
https://arax.rtx.ai/rtxcomplete/nodeslike?word=test\" UNION SELECT sqlite_\
```

The server will return JSON in the HTTP response, with the SQLite version as "3.11.0" as part of the first item in the array:

```
jQuery331058383639737050O6_1650064361901([{"curie": "??", "name": "3.11.0",
```

Impact

This vulnerability is critical as it can lead to remote code execution and thus complete server takeover.

References

- Vulnerable endpoint with PoC SQL injection payload

CVE
CVE-2022-1531
(Published)

Vulnerability Type
CWE-89: SQL Injection

Severity
Critical (10)

Registry
Other

Affected Version
All

Visibility
Public

Status
Fixed

Found by

Jordan Sherman
@deleterepo
legend

This report was seen 658 times.

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

We created a **GitHub Issue** asking the maintainers to create a `SECURITY.md` 7 months ago

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

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

Thank you for reporting this issue. We have created a SECURITY.md file per your suggestion sent

via email. We are working on a fix for this issue. Thank you for keeping the issue private until we have had a chance to fix it.

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

Thank you, we have fixed the issue with commit https://github.com/RTXteam/RTX/commit/fa2797e656e3dba18f990a2db1f0f029d41f1921

Thank you for reporting this issue to our team.

Jordan Sherman 7 months ago Researcher

Thanks for the update @maintainer! @admin can we get a CVE for this?

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

Jamie Slome 7 months ago Admin

@maintainer - are you able to mark as valid and fixed using the resolve button below?

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

Hi Jordan, what is a CVE? Please pardon my ignorance.

Jordan Sherman 7 months ago Researcher

Hi @maintainer. No problem, happy to help. A CVE is simply an ID for this vulnerability. The mission of the CVE Program is to identify, define, and catalog publicly disclosed cybersecurity vulnerabilities. There is one CVE Record for each vulnerability in the catalog. The vulnerabilities are discovered then assigned and published by organizations from around the world that have partnered with the CVE Program, such as this platform (Huntr). Please see here for more info: https://www.cve.org/About/Overview

Jamie Slome 7 months ago Admin

Just for further clarity, we take care of the entire CVE process for you, so there is nothing for you to do, except give us the go-ahead to publish one 👍

A rtxteam/rtx maintainer 7 months ago

Thank you, Jordan. It turns out we have deployed the fix to one of our two production servers. Deployment to another production server involves coordinating with a federal agency (NIH) and may take a few days. Thank you for your patience.

Jamie Slome 7 months ago Admin

👍

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

Hi Jordan and Jamie, OK, I have confirmed that the patch was also deployed to the NIH's servers, and thus, we are ready to resolve this issue. Thank you for your patience, and big thank you for reporting this security vulnerability through the huntr.dev program.

A rtxteam/rtx maintainer validated this vulnerability 7 months ago

Jordan Sherman 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_2022-04-20 with commit fa2797
7 months ago

The fix bounty has been dropped ✖

This vulnerability will not receive a CVE ✖

Jamie Slome 7 months ago Admin

Great work to all involved! 👍

A CVE has been assigned and should be published shortly. More generally, this makes the rtxteam look like they take security seriously and are doing a great job at resolving security

issues :)

> Sign in to join this conversation