# Cross Site Request Forgery in profile's "SSH Keys" leads to unauthorized access to the system in ikus060/rdiffweb

0

Valid Reported on Sep 14th 2022

## Description

While adding SSH public keys to the profile, the server accepts the GET request which results in adding an SSH public key to the profile and leads to unauthorised access to the system and backups.

## Proof of Concept

Open the below url after logging in to the demo site.SSH Public key will be added to the profile.

```
https://rdiffweb-demo.ikus-soft.com/prefs/sshkeys?action=add&title=ssh1&key
```

OR

1 - On burpsuite, capture the SSH public key adding request and right click and click on change request method , it will change the POST request method to GET after that right click and Copy that URL.
2 - Login to the demo site and open that copied URL. SSH key will add to the account.

## Impact

Unauthorized access to the system and backups.

## References

- https://guides.codepath.com/websecurity/Cross-Site-Request-Forgery#:~:text=the%20user's%20browser.-,CSRF%20GET%20Request,or%20in%20a%20phishing%20

CVE
CVE-2022-3221
(Published)

Vulnerability Type
CWE-352: Cross-Site Request Forgery (CSRF)

Severity
High (8.8)

Registry
Pypi

Affected Version
2.4.2 and below

Visibility
Public

Status
Fixed

Found by

Ambadi MP
@ciph0x01
legend

Fixed by

Patrik Dufresne
@ikus060
unranked

This report was seen 686 times.

We are processing your report and will contact the **ikus060/rdiffweb** team within 24 hours.
2 months ago

**Ambadi MP** modified the report 2 months ago

A **ikus060/rdiffweb** maintainer has acknowledged this report 2 months ago

**Patrik Dufresne** validated this vulnerability 2 months ago

Ambadi MP has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

Patrik Dufresne 2 months ago Maintainer

@admin Is it possible to create a CVE ? Thanks

Patrik Dufresne marked this as fixed in 2.4.3 with commit 9125f5 2 months ago

Patrik Dufresne has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ✖

Jamie Slome 2 months ago Admin

Done 👍

Sign in to join this conversation