IP whitelist bypass #2761

Closed **bstapes** opened this issue on Apr 2, 2020 · 1 comment

bstapes commented on Apr 2, 2020 • edited

Teampass includes a feature to restrict the source IP address users can use to interact with Teampass. The value of the source IP address is defined from the first value in the X-Forwarded-For header in the client request.

Due to the fact that the client controls the X-Forwarded-For header and can set it to any value of their choosing, this header can be set to a whitelisted value which allows any client that can guess a whitelisted IP address to interact with Teampass from wherever they like.

Steps to reproduce

1. Add 1.1.1.1 to the list of API IP Addresses allowed
2. Make an API call with an appropriate X-Forwarded-For header and notice that the call is valid

```
curl -v -H "X-Forwarded-For: 1.1.1.1" http://localhost/teampass/api/index.php/info/version/?apikey=xyz
```

Steps to fix

- No data in headers provided by the client can be trusted, including X-Forwarded-For.
- The only reliable data about a client IP address is in the Source Address field in a TCP packet (details).

Server configuration

Teampass version:
2.1.27.36

lochiiconnectivity commented on Apr 28, 2021

The feature of which you speak was introduced in #1559 - the assumption here is that the application is deployed behind a sanitising proxy which does not permit the user to control the XFF header.

Perhaps the solution here is to allow the administrator to choose if XFF is honoured in the installation or not.

nilsteampassnet closed this as completed on Oct 31

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

3 participants