New issue

Jump to bottom

FVP-02-011 API: Information disclosure via device endpoint #806

Closed **bakulf** opened this issue on Apr 7, 2021 · 1 comment

Labels p3

bakulf commented on Apr 7, 2021 • edited by data-sync-user Collaborator

It was found that the corresponding API used by the Mozilla VPN applications includes sensitive information into response messages in case an error is triggered. The backend speaks to the Mullvad partner API which handles account-related data for each Mozilla VPN user. However, if the Mullvad API throws an error, the backend includes this message in the response and returns it to the client. This might lead to an exposure of sensitive data, such as the corresponding Mullvad account ID, as shown below. Adversaries would be able to leverage this sort of information to perform further attacks against the connected APIs.

```
Affected Request:
POST /api/v1/vpn/device HTTP/1.1
Host: stage-vpn.guardian.nonprod.cloudops.mozgcp.net
Content-Type: application/json
Authorization: Bearer [...]
{"name":"from-wireguard-
conf","pubkey":"T1fKJp8knv4kqsfy9O04OIy+1nl5b9ypcnIzdmcfyzM="}

Response:
HTTP/1.1 500 Internal Server Error
Date: Wed, 31 Mar 2021 08:56:57 GMT
[...]

{"message":"https://partner.mullvad.net/v1/accounts/
b018d34efd734a27a06e155756733c8b/wireguard-keys/ returned unexpected
statusCode=400, body={\"code\":\"RELAY_PUBKEY\",\"error\":\"WireGuard public key
in use by a relay\"}, taskType=ADD_DEVICE"}
```

It is recommended not to route error messages received from the Mullvad partner API back to the client. Instead, a static error message or an error identifier should be employed to be able to monitor the application.

┆ Issue is synchronized with this Jira Task

bakulf added p3 **audit-issue** labels on Apr 7, 2021

bakulf self-assigned this on Apr 8, 2021

bakulf commented on Apr 8, 2021 Collaborator Author

mozilla-services/guardian-website#1106

bakulf closed this as completed on Apr 9, 2021

data-sync-user unassigned **bakulf** on Aug 11, 2021

Assignees

No one assigned

Labels

p3

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant