Jump to bottom

## Manipulation of Host Header lead to Account Takeover Vulnerability #748



New issue

○ Closed mdisec opened this issue on Mar 23, 2020 · 11 comments

bug interface security Labels

mdisec commented on Mar 23, 2020 • edited 🕶

Tbh, vulnerability is pretty simple. On line 33. \$\_SERVER['HTTP\_HOST'] value is directly used without any validation and then on line 34. E-mail send to the targeted account's email address.

hestiacp/web/reset/index.php

\$mailtext .= \_\_('PASSWORD\_RESET\_REQUEST',\$\_SERVER['HTTP\_HOST'],\$user,\$rkey,\$\_SERVER['HTTP\_HOST'],\$user,\$rkey);

Content of the password reset e-mail is generated by using following string definition.

'PASSWORD\_RESET\_REQUEST' => "To reset your control panel password, please follow this link:\nhttps://\s/reset/?action=confirm&user=\s&code=\s\n\nAlternatively, you may go\_winttps://\s/reset/?action=code&user=\s and \text{ the following reset\_oci:\nhs\n\nTf you did not request password reset, please ignore this message and accept our apologies.\n\n—\nVesta Control Panel\n",

Host header value used for URL

generation !!!

Pass reset token

So that means, \$\_SERVER['HTTP\_HOST'] value is used for URL generation in e-mail template and we can fully control it.

We can spoof \$\_SERVER['HTTP\_HOST']value during HTTP request to the password reset endpoint.

Actual Host header value IS NOT hacker com but the URL will be hacker com in the password reset e-mail. As you can following screenshot, even though the Vesta is being installed on 192.168.74.163 on port 8060, URL placed in the e-mail for account recovery is HACKER.com now. So if the admin user click on that link in the e-mail, HACKER.COM will steal the code value which is enough for resetting password of the admin user.

PS: I should mention that in the real-life use-case you can very similar domain name instead of hacker.com:) Since the e-mail is being sanded from Vesta server, it's not a kind of phishing attack.

## Vesta Control Panel

Password Reset at 2020-03-11 16:22:06

To: Mehmet INCE

16 user=admin

Hello, System Administrator,
To reset your entrol panel password, please follow this link:
https://hacker.com/reset/?action=confirm&user=admin&code=U06sNrASFC

Alternatively, you may go to <a href="https://hacker.com/reset/?action=code&user=admin">https://hacker.com/reset/?action=code&user=admin</a> and enter the following reset code: U06sNrASFC

If you did not request password reset, please ignore this message and accept our apologies.

Vesta Control Panel

## Suggested Fix

According to technical details of the installation, Vesta installs it's own Apache, Nginx and bunch of services. That means %90 of the real-life deployment is standalone server. By saying that I mean, there is no different service in front of the Vesta where might be validation on Host field of request header.

This vulnerability could have been mitigated by doing Nginx configuration, which is being used as reverse-proxy in the product, or even can be Apache without touching PHP side. But default Vesta configuration gives your chance to work with Host field.

## Side Note

I've found & successfully tested that vulnerability during analysis of Vesta! I haven't tested it against HestiaCp but I strongly believe it's also works too



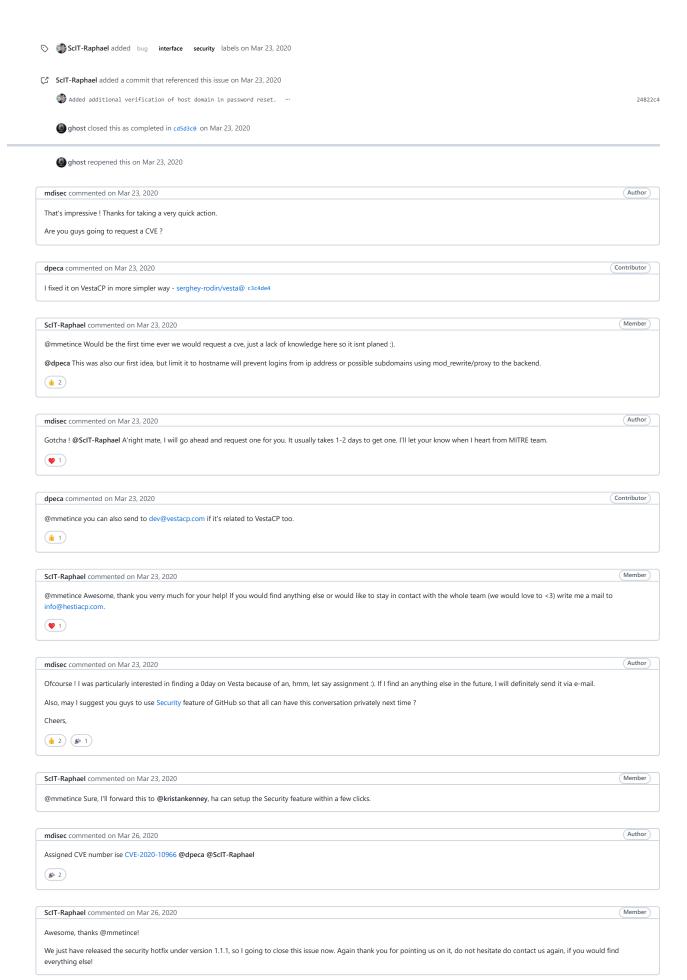
ScIT-Raphael commented on Mar 23, 2020

Member

Hi @mmetince

Thank you for pointing us on this serious issue! We're currently working on a fix and will release a new version asap.





Assignees
No one assigned
Labels
bug interface security
Projects
None yet
Milestone
No milestone
Development
No branches or pull requests

3 participants

