CVE-2021-27231 - Hestia Control Panel 1.4.0 and below - Subdomain Takeover - Improper Privilege Management

by Sick Codes — May 12, 2021 in Security 2

Title

Hestia Control Panel 1.4.0 and below - Subdomain Takeover - Improper Privilege Management

CVE ID

CVE-2021-27231

CVSS Score

5.4

CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N

Internal ID

SICK-2021-006

Vendor

Hestia Control Panel

Product

Hestia Control Panel

Product Versions:

HestiaCP Debian 9 v1.4.0 and below

HestiaCP Debian 10 v1.4.0 and below

HestiaCP Ubuntu 16.04 LTS v1.4.0 and below

HestiaCP Ubuntu 18.04 LTS v1.4.0 and below

HestiaCP Ubuntu 20.04 LTS v1.4.0 and below

Vulnerability Details

A vulnerability in the Hestia Control Panel (HestiaCP) allows remote authenticated attackers on the same shared hosting environment to create domain aliases, or nginx vhosts, for subdomains that belong to other users. For example, an attacker on the same shared hosting service can perform subdomain takeover by creating an alias for a mail domain belonging to another user, resulting in all IMAP and POP requests going to the attacker's account.

Vendor Response

Vendor patched.

Proof of Concept/Exploit

```
BIND9 is not required.

user1 creates just a MAIL service
http://domain.com

user2 creates just a DOMAIN service (insufficient validation of root domain ownership)
http://test.domain.com

user2 can add vhost/alias:
http://domain.com
```

http://webmail.domain.com
http://mail.domain.com

Notably, user2 cannot add vhost/alias http://domain.com.

Results:

Stolen by user2
https://webmail.domain.com
We're working on it!
This site is currently under construction.
Please check back soon.
Domain: http://test.domain.com

Stolen by user2
https://mail.domain.com
We're working on it!
This site is currently under construction.
Please check back soon.
Domain: http://test.domain.com

user1's email account details are all stolen by user2
Username:
info@domain.com
Password:
IMAP Hostname: http://mail.domain.com
SMTP Hostname: http://mail.domain.com
Webmail Alias: http://webmail.domain.com

- open webmail button in user1's email domain leads to user2's takeover.
- user2 can subsequently phish user1 at the webmail domain.
- user2 can steal credentials on next IMAP/POP request, e.g. mobile phone refresh emails.
- complete denial of service of user1's email accessibility
- complete email account takeover
- phishing the account for 1 stolen credential request, and then reverting the theft, will then allow user2 to access user1's emails.

DNS
@   ip.address
@www
            ip.address
@mail
           ip.address
@webmail
        ip.address
MX @   http://mail.domain.com

Original Issue by @ir_kujoe https://twitter.com/ir_kujoe

[BUG] Any user can create a subdomain for any domain using the HestiaCP DNS server even for other users. #1622

Describe the bug
Any user can create a subdomain for any domain on the server and create content using that domain. The Add Web Domain button does not validate whether or not the domain created is a subdomain for a domain already on the server. If user1 owns domain1.com and uses the nameservers for the HestiaCP server, user2 on the same server can create any subdomain for domain1.com and upload any content they want and act like they own the domain. As long as both users are on the same server and the domain is being managed by the same DNS server. This can be a problem for shared hosting environments. Additionally users can send e-mail from this subdomain which would appear legitimate for most e-mail clients since the SPF and DKIM records would be valid.

To Reproduce
What steps did you take when the issue occured?

    Point domain to the HestiaCP server using the nameservers.
    Add the TLD to one user using the Add Web Domain.
    Add a subdomain of the TLD to another user using the Add Web Domain and check "Create DNS Zone".
    View both domains in a browser.

Expected behavior
Throw an error if the user tries to add a subdomain using the Add Web Domain form if the TLD exists for another user (alternatively make a checkbox to enforce this or not).

NOTE: Please do not enforce this for command line and API calls since some shared hosts give out free subdomains. Enforcing this at a user level (i.e. the PHP form) would be a better option.

Operating system:
Ubuntu 20.04 LTS

Hestia Control Panel version:

v1.3.2

Additional context
DirectAdmin has added a checkbox to their settings for this, might be a better solution:
image
(Link to DA feature request for further info: https://www.directadmin.com/features.php?id=925)

For additional reference, here's an old thread from VestaCP with 2 possible solutions (mine being the worst of the 2):
https://forum.vestacp.com/viewtopic.php?f=13&t=9175

Links

https://sick.codes/sick-2021-006

https://github.com/sickcodes/security/blob/master/advisories/SICK-2021-006.md

https://github.com/hestiacp/hestiacp/issues/1622

Disclosure Timeline

- **2021-02-15** - Researchers discover vulnerability.
- **2021-02-15** - Vendor notified.
- **2021-02-16** - CVE assigned CVE-2021-27231.
- **2021-05-12** - Advisory published.

Researchers

Sick Codes: https://github.com/sickcodes || https://twitter.com/sickcodes

KuJoe: https://github.com/KuJoe || https://twitter.com/ir_kujoe

CVE Links

https://sick.codes/sick-2021-006

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-27231

https://nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-27231

Comments 2

Pingback: Vulnerabilidad en Control Panel (Hestiacp) - CVE-2021-27231 - Información y Soluciones

Rosmary Molina 1 year ago

That was something I and a few others need to know. Both my phone's have been completely taken over and I let Gmail and still I get nowhere. Both phones are about a week old. I'm glad I've been doing my research and thank you very much for the help and information. Please continue to do what you do best. My love Rosemary Molina

Reply

Leave a Reply

Your email address will not be published. Required fields are marked *

Comment *

Name

Email

Website

Privacy - Terms

I am human

POST COMMENT

@sickcodes

@sickcodes

@sickcodes

Discord Server

sickcodes.slack.com

t.me/sickcodeschat

./contact_form