

New issue

Jump to bottom

URL open redirect leads to phishing attacks #4061

Closed naivekun opened this issue on Apr 24, 2020 · 5 comments

Assignees
Labels cleanup
Projects 20.7
Milestone 20.7

naivekun commented on Apr 24, 2020 • edited

Important notices

Before you add a new report, we ask you kindly to acknowledge the following:

[x] I have read the contributing guide lines at <https://github.com/opnsense/core/blob/master/CONTRIBUTING.md>

[x] I have searched the existing issues and I'm convinced that mine is new.

Describe the bug

Redirect URL in login page was not filtered and can redirect user to any website.

Attackers can send a URL like `https://<FIREWALL_IP>?url=http://phishing-site.com/` to firewall user. If user enter the credential and login, he will be redirected to malicious page

To Reproduce

Steps to reproduce the behavior:

1. Access `https://<FIREWALL_IP>?url=http://example.com`
2. Enter the credential.
3. User was redirected to `http://example.com`

Environment

OPNsense 20.1-amd64

FreeBSD 11.2-RELEASE-p16-HBSD

OpenSSL 1.1.1d 10 Sep 2019

naivekun commented on Apr 24, 2020

Author

`core/src/etc/inc/authgui.inc`

Line 117 in 2a216f9

```
117 header(url_safe("Location: {$_GET['url']}"));
```

fichtner commented on Apr 24, 2020

Member

Can you explain how that differs from clicking the malicious URL itself? Auth step or not, what is the severity assessment?

...

naivekun commented on Apr 24, 2020

Author

Malicious URL itself does not starts with "http://<REAL_IP_ADDRESS>". I'll give you an example.

If someone send you a link like "http://192.168.1.1/?url=http://bit.ly/xxxx", "192.168.1.1" makes user feel safe instead of "http://bit.ly/xxxx" and users are more likely to click a URL contains a trusted domain or IP address.

referrer: <https://cwe.mitre.org/data/definitions/601.html>

naivekun commented on Apr 25, 2020

Author

Another reasonable payload is like `http://192.168.1.1/?url=http://csrf_token_XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX.hacker.com` which is more easily to obfuscate user.

`csrf_token_XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX` is a fake subdomain of hacker.com.

AdSchelevis self-assigned this on Apr 26, 2020

AdSchelevis closed this as completed in `0d07fae` on Apr 26, 2020


AdSchelevis added the `cleanup` label on Apr 26, 2020

AdSchelevis commented on Apr 26, 2020

Member

`0d07fae` should prevent off site redirects.

fichtner added this to To do in 20.7 via `automation` on Apr 27, 2020

🔗  **fichtner** added this to the **20.7** milestone on Apr 27, 2020

📋  **fichtner** moved this from **To do** to **Done** in **20.7** on Apr 27, 2020

🗨️  **Akokonunes** mentioned this issue on Jan 7

Create CVE-2020-23015.yaml projectdiscovery/nuclei-templates#3502

🔗 Merged

Assignees

 **AdSchellevis**

Labels

cleanup

Projects

No open projects

1 closed project ▾

Milestone

20.7

Development

No branches or pull requests

3 participants

