Multiple Open Redirect in nitely/spirit

0

Valid Reported on Feb 20th 2022

Description

In the /user/login endpoint, it doesnt check the value of the next parameter when the user is logged in and pass it directly to redirect which result to open redirect. The bug also exist in /user/logout, /user/register, /user/login, /user/resend-activation.

Proof of Concept

```
1. Go to http://127.0.0.1:8000/user/login/?next=https://evil.com
```

Impact

This bug result to open redirect.

Occurrences

views.py L138 views.py L76 views.py L96 views.py L65

CVE
CVE-2022-0869
(Published)

Vulnerability Type
CWE-601: Open Redirect

Severity
Medium (4.3)

Visibility
Public

Status

Fixed

Found by

noobexploiterhuntrdev

@noobexploiterhuntrd...

unranked

This report was seen 607 times.

We are processing your report and will contact the **nitely/spirit** team within 24 hours.
9 months ago

noobexploiterhuntrdev modified the report 9 months ago

We created a **GitHub Issue** asking the maintainers to create a `SECURITY.md` 9 months ago

We have contacted a member of the **nitely/spirit** team and are waiting to hear back
9 months ago

nitely validated this vulnerability 9 months ago

noobexploiterhuntrdev has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

nitely 9 months ago — Maintainer

I fixed this (https://github.com/nitely/Spirit/pull/308), thanks for reporting

noobexploiterhuntrdev 9 months ago — Researcher

Awesome, Thanks, Hi @admin , could i request a cve for this bug?

Jamie Slome 9 months ago — Admin

Once the fix has been confirmed, and if the maintainer is happy for one to be
go ahead and publish a CVE.

@maintainer - could you please `confirm fix` and let us know if you are happy to assign a CVE for

@maintainer could you please `confirm fix` and let us know if you are happy to assign a CVE for this report?

We have sent a fix follow up to the **nitely/spirit** team. We will try again in 7 days. 9 months ago

We have sent a second fix follow up to the **nitely/spirit** team. We will try again in 10 days. 9 months ago

nitely marked this as fixed in **0.12.3** with commit **8f32f8** 9 months ago

The fix bounty has been dropped ✗

This vulnerability will not receive a CVE ✗

views.py#L76 has been validated ✓

views.py#L65 has been validated ✓

views.py#L138 has been validated ✓

views.py#L96 has been validated ✓

nitely 9 months ago — Maintainer

Hi -- done. You can assign a CVE if you want. Thanks again!

noobexploiterhuntrdev 9 months ago — Researcher

hi @admin

Jamie Slome 9 months ago — Admin

Assigned and published! 🎉

`CVE-2022-0869`

noobexploiterhuntrdev 9 months ago

Thanks

Sign in to join this conversation