Instantly share code, notes, and snippets.

harsh-bothra / **CVE-2020-23989**

Last active last year

☆ Star

<> Code   Revisions 4   ☆ Stars 2

Cross-Site Scripting in NeDi 1.9C

CVE-2020-23989

```
Product: NeDi - Find IT

CVE: CVE-2020-23989

Version: 1.9C

Vulnerability: Reflected Cross-Site Scripting

Vulnerability Description:  NeDi 1.9C allows Cross-Site Scripting via "oid" parameter at "pwsec.php" page.

# Steps to Reproduce

1. Log in to the application with provided credentials.
2. Navigate to "https://<nedi_server_ip>/pwsec.php" page.
3. Add "oid" parameter at the end of the URL with XSS Payload like below:
> https://<nedi_server_ip>/pwsec.php?oid=<img src=x onerror=alert(document.domain)>
4. Observe that the XSS Payload provided in Step-3 is executed.

```

NicoleG25 commented on Nov 3, 2020

Hi could you be more specific as to why you think Nedi is vulnerable? I can't seem to find the file you are specifying in https://github.com/NeDi-FindIt/nedi

harsh-bothra commented on Nov 3, 2020 Author

Hi. Please download and deploy this: https://www.nedi.ch/download/ & further you will find this endpoint vulnerable. Let me know if you still face issues to reproduce it.

Peithon commented on Jan 26, 2021

Hi. Why did I not see your feedback record in the CMS issue, but you have successfully applied for a CVE number, and your gist address is in References. How did this happen? Looking forward to receiving your reply.

harsh-bothra commented on Jan 27, 2021 Author

Hi. I am not sure which CMS Record you are referring to. I have reported the issue via Mitre to get this into the light.

Peithon commented on Jan 27, 2021

> Hi. I am not sure which CMS Record you are referring to. I have reported the issue via Mitre to get this into the light.

Hi.I am glad to receive your reply. I apologize for not expressing my question. I want to submit some vulnerabilities to CVE recently, so I took the liberty to ask you for advice. First of all, I am at https://github.com /NeDi-FindIt/nedi/issues did not see that you have any relevant vulnerability feedback records, so I am curious how you reported the vulnerability; secondly, the CVE number is http://cve.mitre.org/cgi-bin/cvename.cgi ?name=CVE-2020-23989, the creation time of the gist address of the References information is later than the CVE number allocation time, how is this done? Your reply will solve a lot of my doubts, looking forward to your reply

harsh-bothra commented on Jan 28, 2021 Author

> > Hi. I am not sure which CMS Record you are referring to. I have reported the issue via Mitre to get this into the light.
>
> Hi.I am glad to receive your reply. I apologize for not expressing my question. I want to submit some vulnerabilities to CVE recently, so I took the liberty to ask you for advice. First of all, I am at https://github.com /NeDi-FindIt/nedi/issues did not see that you have any relevant vulnerability feedback records, so I am curious how you reported the vulnerability; secondly, the CVE number is http://cve.mitre.org/cgi-bin/cvename.cgi ?name=CVE-2020-23989, the creation time of the gist address of the References information is later than the CVE number allocation time, how is this done? Your reply will solve a lot of my doubts, looking forward to your reply

When we submit an issue through MITRE (you can either approach to the vendor or go through MITRE for open-source projects), we also provide a working proof of concept/steps to reproduce the issue while submitting it to MITRE. The team further verifies and assigns a CVE Number. Now, in order to publish the CVE, you need to provide a PoC through GitHub or something which is later published. Also, sometimes the CVE no. is blocked based on the vendor as well. In this case, the CVE was requested about 3 months before it was allocated. After which it was asked to provide the details which were shared through this GIST. This is the reason you are seeing the difference in publication dates. I hope it clarifies your doubts.

Peithon commented on Jan 28, 2021

> > > Hi. I am not sure which CMS Record you are referring to. I have reported the issue via Mitre to get this into the light.

> > Hi.I am glad to receive your reply. I apologize for not expressing my question. I want to submit some vulnerabilities to CVE recently, so I took the liberty to ask you for advice. First of all, I am at https://github.com /NeDi-FindIt/nedi/issues did not see that you have any relevant vulnerability feedback records, so I am curious how you reported the vulnerability; secondly, the CVE number is http://cve.mitre.org/cgi-bin/cvename.cgi ?name=CVE-2020-23989, the creation time of the gist address of the References information is later than the CVE number allocation time, how is this done? Your reply will solve a lot of my doubts, looking forward to your reply
>
> When we submit an issue through MITRE (you can either approach to the vendor or go through MITRE for open-source projects), we also provide a working proof of concept/steps to reproduce the issue while submitting it to MITRE. The team further verifies and assigns a CVE Number. Now, in order to publish the CVE, you need to provide a PoC through GitHub or something which is later published. Also, sometimes the CVE no. is blocked based on the vendor as well. In this case, the CVE was requested about 3 months before it was allocated. After which it was asked to provide the details which were shared through this GIST. This is the reason you are seeing the difference in publication dates. I hope it clarifies your doubts.

Thanks, this is very helpful to me