Instantly share code, notes, and snippets.

# UditChavda / CVE-2022-40895

Last active 2 months ago

☆ Star

<> Code    -O-Revisions 4

CVE-2022-40895

<> CVE-2022-40895

```
> Product : NeDi

> CVE : CVE-2022-40895

> version : NeDi 1.0.7

> Vulnerability : Observable Discrepancy

> Vulnerability Description : In certain Nedi products, a vulnerability in the web UI of NeDi logi
                              Community login could allow an unauthenticated, remote attacker to
                              affect the integrity of a device via a User Enumeration vulnerabilit
                              The vulnerability is due to insecure design, where a difference in
                              forgot password utility could allow an attacker to determine if the
                              user is valid or not, enabling a brute force attack with valid users
                              This affects NeDi 1.0.7 for OS X 1.0.7 <= and NeDi for Suse 1.0.7 <=
                              and NeDi for FreeBSD 1.0.7 <= & community login page.


> Additional Information : A vulnerability in the web UI of NeDi login & Community login could all

> Remediation : The Password reset utility should have generic/common message as output to mitigat


> Affected Component : Community Login of NeDi, personal hosted login of NeDi

> [Impact Information Disclosure]
  true


# Steps to Reproduce
 1)Open NeDi Login or use NeDi Community login.
 2)Click on Forgot Password
 3)Brute Force the email id - it will respond with " There are no usernames associated with that e

# [Reference]
> http://forum.nedi.ch/index.php
> https://www.nedi.ch/
```