Code Injection in publify/publify

Valid Reported on Feb 10th 2022

0

Description

The application doesn't check/filter the comments provided by the user before save to database. Attacker can't insert js code to steal admin's data but can insert html code, leads to many information security risks.

Proof of Concept

Step 1: Go to https://demo-publify.herokuapp.com/2022/02/11/hello-world#comments and comment in anonymous user.

```
<img src=https://www.technistone.com/color-range/image-slab/Starlight%20Bla
```

Step 2: Login as demo user, go to https://demo-publify.herokuapp.com/admin/feedback. You can see html code has been rendered successfully.
PoC: https://drive.google.com/file/d/1RSuq7fsyJPrbNHqlZ9pRW3lgXAvmOrQf

Impact

Attacker can insert html code to break the website format, phishing or collect the admin's IP through loading images in img tags.

CVE
CVE-2022-0578
(Published)

Vulnerability Type
CWE-94: Code Injection

Severity
Medium (5.3)

Visibility
Public

Status
Fixed

Found by

nhiephon
@nhiephon
master

Fixed by

Matijs van Zuijlen
@mvz
maintainer

This report was seen 527 times.

We are processing your report and will contact the **publify** team within 24 hours. 10 months ago

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

Matijs van Zuijlen validated this vulnerability 9 months ago

nhiephon has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

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

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

Matijs 9 months ago

A fix has been merged and will be released soon.

We have sent a third and final fix follow up to the **publify** team. This report is now considered

We have sent a third and final fix follow up to the **publify** team. This report is now considered stale. 9 months ago

Matijs van Zuijlen marked this as fixed in **9.2.8** with commit **b50df0** 6 months ago

Matijs van Zuijlen has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ✖

Sign in to join this conversation