huntr

Leaking password protected articles content due to improper access control in publify/publify

0

✓ Valid Reported on Apr 10th 2022

Description

Any user who can publish their article can protect it using a password before publishing. So, a valid password to the article is required to view the contents of the article. But when a request is made to article /2022/04/10/<article-title> the UI show it requires a password to view content. But the content of the article is leaked in meta tags of the response.

Proof of Concept

Steps to Reproduce:
Login to app as Admin and create an article and protect it with a password and publish it
Now, login as a demo user and navigate to the newly published article. You can see the UI shows it requires a password to view.
But the content of the article is already leaked in the meta tags of the response body

Impact

Attackers can leverage this vulnerability to view the contents of any password-protected article present on the publify website. compromising confidentiality and integrity of users.

CVE
CVE-2022-1553
(Published)

Vulnerability Type
CWE-284: Improper Access Control

Severity
High (8.8)

Registry
Other

Chat with us

Affected Version

Publify 9.2.7

Visibility

Public

Status

Fixed

Found by

Mahendra Thanniru

@mah1ndra

unranked

Fixed by

Matijs van Zuijlen

@mvz

maintainer

This report was seen 522 times.

We are processing your report and will contact the **publify** team within 24 hours. 8 months ago

We have contacted a member of the **publify** team and are waiting to hear back 8 months ago

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

We have sent a second follow up to the **publify** team. We will try again in 10 days. 7 months ago

We have sent a third and final follow up to the **publify** team. This report is now considered stale. 7 months ago

A **publify/publify** maintainer has acknowledged this report 7 months ago

Matijs van Zuijlen validated this vulnerability 7 months ago

I can reproduce this, thanks!

Chat with us

Mahendra Thanniru has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

Mahendra 7 months ago

Researcher

Hi Matijs, I've more vulnerability to report and discuss. Can you please share me a contact where I can reach out quickly without this long delay? i really excited to work with you.

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

We have sent a second fix follow up to the **publify** team. We will try again in 10 days. 6 months ago

Matijs 6 months ago

Hi Mahendra, this platform is the quickest way to reach me.

Matijs van Zuijlen marked this as fixed in **9.2.8** with commit **1a78f1** 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

2022 © 418sec

Chat with us