Cross-site Scripting (XSS) - Stored in meetecho/janus-gateway

0

Valid Reported on Nov 22nd 2021

Description

an user can enter a text room in janus gateway with a malicious name that contains a xss payload and could poison other users on the room

Proof of Concept

just go to https://janus.conf.meetecho.com/textroomtest.html this is provided by github repo as a demo
then enter in the name `<img src=x onerror=alert(document.domain)>`

POC video :

https://drive.google.com/file/d/1r8oy-BFGV_Z1WICyQnR_c5Nq4CAfxWuE/view?usp=sharing

Impact

This vulnerability is capable of poison the whole chat and steal other users creds or redirect users to malicious apps.

CVE
CVE-2021-4020
(Published)

Vulnerability Type
CWE-79: Cross-site Scripting (XSS) - Stored

Severity
High (8.8)

Visibility
Public

Status
Fixed

Found by

Soufiane El Habti
@soufelhabti
unranked

This report was seen 449 times.

We are processing your report and will contact the **meetecho/janus-gateway** team within 24 hours. a year ago

We created a **GitHub Issue** asking the maintainers to create a `SECURITY.md` a year ago

We have contacted a member of the **meetecho/janus-gateway** team and are waiting to hear back a year ago

A **meetecho/janus-gateway** maintainer a year ago

Thanks for the explaination! This is Lorenzo, main author of Janus.

Looking at the details, this sounds more like an issue with the sample demo page, rather than a problem in the Janus server codebase instead. We do have some escaping for messages, but we indeed forgot to do the same for display names (which as you pointed out are inserted in the HTML code directly too), so this *should* be an easy fix.

Unless you think this is more of an issue in the server side instead, which allows such IDs to be used in the first place? In fact, while it's easy for us to fix it in our demo, there may be other implementations doing something similar and not knowing this might be an issue: limiting the scope of display names would help here, but could be overly constraining. As an alternative, we can simply add some documentation for the plugin that explains this can happen.

A **meetecho/janus-gateway** maintainer a year ago

As a side note, what's the proper etiquette when submitting patches to fix the problem? Creating a pull request that describes the issue and the fix, and crediting the reporter? Thanks!

Soufiane a year ago Researcher

I confirm there s no issue with server side only on client side where the payload is executed, glad to hear from your side good luck for the fix

Soufiane a year ago Researcher

You can refer to this issue https://github.com/netbox-community/netbox/issues/7788
I guess the same process is followed by everyone

A **meetecho/janus-gateway** maintainer a year ago

Ack, will do it, thanks! I'm working on a patch right now, so it should hopefully be ready soon.

A **meetecho/janus-gateway** maintainer validated this vulnerability a year ago

Soufiane El Habti has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

A **meetecho/janus-gateway** maintainer marked this as fixed in **0.11.6** with commit **d3fc00** a year ago

The fix bounty has been dropped ×

This vulnerability will not receive a CVE ×

Sign in to join this conversation