Cross-site Scripting (XSS) - Stored in invoiceninja/invoiceninja

0

Valid Reported on Nov 17th 2021

Description

In recent InvoiceNinja version (9d7145c) in /documents it is possible to store svg file with html/js content, which later can be used to phish other users

Proof of Concept

```
POST /documents HTTP/1.1
Host: 172.17.0.1:8888
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:95.0) Gecko/20100101 Firefox
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=---------------------------3009
Content-Length: 4489
X-CSRF-TOKEN: XSsl95vSUFGZZo1G6B3sykTJTQdhNhtQnqtjoAax
X-Requested-With: XMLHttpRequest
Content-Length: 4489
Origin: http://172.17.0.1:8888
DNT: 1
Connection: close
Referer: http://172.17.0.1:8888/invoices/1/edit
Cookie: XSRF-TOKEN=eyJpdiI6Ik52dWlvNzlXbEpmU3RvbW1uS1Nsc0E9PSIsInZhbHVlIjoi

-----------------------------300959455021219094302820715478
Content-Disposition: form-data; name="_token"

VUGoBgaUdmFPvl3XRKJLUaLJc5ETKEkhGinTNE3t
-----------------------------300959455021219094302820715478
Content-Disposition: form-data; name="file"; filename="ssa.svg"
Content-Type: text/html

[PHISHING_CONTENT_CODE]
-----------------------------300959455021219094302820715478--
```

After this You can visit url received in response
http://172.17.0.1:8888/documents/{document_id}

Impact

FROM OWASP:: An attacker can use XSS to send a malicious script to an unsuspecting user. The end user's browser has no way to know that the script should not be trusted, and will execute the script. Because it thinks the script came from a trusted source, the malicious script can access any cookies, session tokens, or other sensitive information retained by the browser and used with that site.

Sample SVG file

https://pastebin.com/h7XTxpi3

CVE
CVE-2021-3977
(Published)

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

Severity
Medium (6.5)

Visibility
Public

Status
Fixed

Found by

theworstcomrade
@theworstcomrade
unranked

Fixed by

theworstcomrade
@theworstcomrade
unranked

This report was seen 387 times.

We are processing your report and will contact the **invoiceninja** team within 24 hours. a year ago

We have contacted a member of the **invoiceninja** team and are waiting to hear back a year ago

David Bomba validated this vulnerability a year ago

theworstcomrade has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

theworstcomrade submitted a **patch** a year ago

David Bomba a year ago — Maintainer

Thanks for this, this repo is in maintenance only mode, I think the best option here is to remove .svg from the acceptable file upload types.

theworstcomrade a year ago — Researcher

@turbo124 I have made changes to the patch according to your suggestion

David Bomba a year ago — Maintainer

Thanks, can you PR the change please

theworstcomrade a year ago — Researcher

@turbo124 @admin could You mark it as fixed? As I see PR's are merged
https://github.com/invoiceninja/invoiceninja/pull/6985
https://github.com/invoiceninja/invoiceninja/pull/6986

David Bomba a year ago — Maintainer

@theworstcomrade

We can't fill in the entire form of the FIx, because it requires a release tag which has not been created yet.

theworstcomrade a year ago — Researcher

@turbo124 @admin it looks like the tags for both branches have already been released
https://github.com/invoiceninja/invoiceninja/releases/tag/v4.5.47
https://github.com/invoiceninja/invoiceninja/releases/tag/v5.3.33

David Bomba marked this as fixed in **v.5.33** with commit **1186ea** a year ago

theworstcomrade has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ✖

Sign in to join this conversation