Unrestricted Upload of File with any dangerous extension in polonel/trudesk

1

Valid Reported on Jun 2nd 2022

Description

Unrestricted Upload of File with any extension

Proof of Concept

```
1. Create a ticket
2. Upload a file with any dangerous extension
3. Intercept the request in Burp Suite, replace the Content-Type with image

POC video:
https://drive.google.com/file/d/1FwS6zC1YaYXBFoPUsTqmjdM1V5buHDT-/view?usp=
```

Impact

Normal user can update a dangerous file that threat to the system
Another users may download the dangerous file

Occurrences

JS tickets.js L703-L716

CVE
CVE-2022-2128
(Published)

Vulnerability Type
CWE-434: Unrestricted Upload of File with Dangerous Type

CWE-434: Unrestricted Upload of File with Dangerous Type

Severity
Critical (9.6)

Registry
Other

Affected Version
<=1.2.3

Visibility
Public

Status
Fixed

Found by

Lê Ngọc Hoa
@lengochoa7112000
master

Fixed by

Chris Brame
@polonel
unranked

This report was seen 724 times.

We are processing your report and will contact the **polonel/trudesk** team within 24 hours. 6 months ago

Lê Ngọc Hoa modified the report 6 months ago

We have contacted a member of the **polonel/trudesk** team and are waiting to hear back 6 months ago

We have sent a follow up to the **polonel/trudesk** team. We will try again in 7 days. 6 months ago

A **polonel/trudesk** maintainer has acknowledged this report 6 months ago

Chat with us

Lê Ngọc Hoa 6 months ago Researcher

Hi @maintainer, I see you read the report. Is it hard to understand or my PoC video does not work? You can ask me something. Thank you!

Lê Ngọc Hoa 6 months ago Researcher

@admin hi admin, can you help me contact to maintainer? Thanks!

Jamie Slome 5 months ago Admin

@lengochoa7112000 - our system will automatically continue to ping the maintainer. Please have patience. This maintainer is usually very active and so you should hear back from them shortly. To see how active they are, feel free to view their repository page:

polonel/trudesk

Chris Brame assigned a CVE to this report 5 months ago

Chris Brame validated this vulnerability 5 months ago

Lê Ngọc Hoa has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

Chris Brame 5 months ago Maintainer

This has been fixed in v1.2.4. I will update this report once it is released.

Chris Brame marked this as fixed in 1.2.4 with commit fb2ef8 5 months ago

Chris Brame has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ✘

tickets.js#L703-L716 has been validated ✔

Sign in to join this conversation

Chat with us