Cross-site Scripting (XSS) - Stored in notrinos/notrinoserp

0

Valid Reported on May 7th 2022

Description

The software does not neutralize or incorrectly neutralizes user-controllable input before it is placed in output that is used as a web page that is served to other users.

Proof of Concept

Add Item,And name is payload (<script>alert(location)</script>).
https://drive.google.com/file/d/148ERIRpfmNDpNXY4X3sW8SqP_UOmute8/view?usp=sharing
Click Item list,xss is executed. https://drive.google.com/file/d/1ITonDK4LRg4fEsL8FY7-1G7dTwIhqlJo/view?usp=sharing
https://drive.google.com/file/d/1eMU6WD6ZZiqCKE9f08iUKFjJo2fRJyeg/view?usp=sharing

Impact

Every user clicking the menu can be affected by malicious javascript code created by the attacker.

CVE
CVE-2022-2871
(Published)

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

Severity
Medium (4.6)

Registry
Other

Affected Version
<=0.7

Visibility

Public

Status

Fixed

Found by

Nick

@nickshadows

unranked

This report was seen 632 times.

We are processing your report and will contact the **notrinos/notrinoserp** team within 24 hours. 7 months ago

We created a **GitHub Issue** asking the maintainers to create a `SECURITY.md` 7 months ago

We have contacted a member of the **notrinos/notrinoserp** team and are waiting to hear back 3 months ago

Phương gave praise 3 months ago

The problem has been reproduced and fixed. Thanks @nickshadows

The researcher's credibility has slightly increased as a result of the maintainer's thanks: +1

Phương validated this vulnerability 3 months ago

Nick has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

Phương marked this as fixed in **0.7** with commit **036277** 3 months ago

The fix bounty has been dropped ✖

This vulnerability will not receive a CVE ✖

Nick 3 months ago Researcher

Nick 3 months ago Researcher

@admin can you pls assign a CVE for this?

Jamie Slome 3 months ago Admin

Same here, happy to proceed with a CVE once we get the go-ahead from the maintainer 👍

Nick 3 months ago Researcher

@maintainer , I would be glad if you could approve for CVE.

Phương 3 months ago Maintainer

Same here, happy to proceed with a CVE once we get the go-ahead from the maintainer 👍

@admin yes please go ahead

Jamie Slome 3 months ago Admin

Sorted 👍

> Sign in to join this conversation