huntr

Cross-site Scripting (XSS) - Reflected in keystonejs/keystone

0

✓ Valid Reported on Dec 30th 2021

Description

On Login Page, There Is A "from=" parameter in URL which is vulnerable to open redirect and which can be escalated to reflected XSS.

Proof of Concept

Install Keystone 6 On Your System.
Go To http://localhost:3000/signin?from=http://evil.com And Login And You'll Be Redirected To evil.com.
Go To http://localhost:3000/signin?from=javascript:alert(document.domain) And Login And After Login, You'll See Two Reflected XSS Pop Ups.

Impact

This vulnerability is capable of making users to redirect to any malicious website using open redirect and reflected XSS can help the attacker to fetch cookies and also for phishing.

Occurrences

TS index.ts L117

References

- https://nvd.nist.gov/vuln/detail/CVE-2018-1000671

CVE
CVE-2022-0087
(Published)

Chat with us

Vulnerability Type

CWE-79: Cross-site Scripting (XSS) - Reflected

Severity

High (7.1)

Visibility

Public

Status

Fixed

Found by

Shivansh Khari

@shivansh-khari

unranked

This report was seen 493 times.

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

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

We have sent a follow up to the **keystonejs/keystone** team. We will try again in 7 days. a year ago

A **keystonejs/keystone** maintainer validated this vulnerability a year ago

Shivansh Khari has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

A **keystonejs/keystone** maintainer a year ago Maintainer

@shivansh-khari we are adding a security advisory and patch release to the GitHub repository soon (hopefully this week), are you OK with us crediting your listed GitHub account https://github.com/shivansh-khari for the CVE?

Shivansh Khari a year ago

Chat with us

Yes Sure You Can Credit My This Github Account With CVE, It Would Be Great.

Thanks

Shivansh Khari a year ago Researcher

@Maintainer Please Let Me Know When You Release A Patch And Credit My Account With CVE, Would Like To Validate The Patch And Help.

A keystonejs/keystone maintainer a year ago Maintainer

Intended release date for patch is today, we will credit your GitHub account

A keystonejs/keystone maintainer a year ago Maintainer

Published at https://github.com/keystonejs/keystone/security/advisories/GHSA-hrgx-7j6v-xj82

Published `@keystone-6/auth` as `1.0.2`

Shivansh Khari a year ago Researcher

Thank You For The Credit, It Was Great Working To Help And Secure Keystone.

Shivansh Khari a year ago Researcher

Also When Will The CVE Will Be Published?

A keystonejs/keystone maintainer marked this as fixed in @keystone-6/auth@1.0.2 with commit 96bf83 a year ago

The fix bounty has been dropped ✗

This vulnerability will not receive a CVE ✗

index.ts#L117 has been validated ✓

A keystonejs/keystone maintainer a year ago

Could the description be updated to what is in

Could the description be updated to what is in
https://github.com/keystonejs/keystone/security/advisories/GHSA-hrgx-7j6v-xj82?

Shivansh Khari a year ago

Researcher

Can't Edit Now, I Guess.

Sign in to join this conversation

huntr

home

hacktivity

leaderboard

FAQ

contact us

terms

privacy policy

part of 418sec

company

about

team

Chat with us