huntr

Cross-Site Request Forgery (CSRF) in phoronix-test-suite/phoronix-test-suite

0

✔ **Valid** Reported on Jan 12th 2022

Description

Hi there, I would like to report another CSRF in phoronix

Proof of Concept

Install a local instance of phoronix
Create a benchmark and note down benchmark id
Access the link `/?benchmark/<benchmark-id>/&repeat` , `/?benchmark/<benchmark-id>/&disable`
and `/?benchmark/<benchmark-id>/&remove` and see that the benchmark is repeated, disabled
and removed.

Impact

This vulnerability is capable of CSRF.

Occurrences

🐘 phoromatic_benchmark.php L110

CVE
CVE-2022-0238
(Published)

Vulnerability Type
CWE-352: Cross-Site Request Forgery (CSRF)

Severity
Medium (4.5)

Visibility

Chat with us

Status
Fixed

Found by

M0rphling
@ktg9

amateur ⌄

We are processing your report and will contact the **phoronix-test-suite** team within 24 hours.
10 months ago

We have contacted a member of the **phoronix-test-suite** team and are waiting to hear back
10 months ago

A **phoronix-test-suite/phoronix-test-suite** maintainer validated this vulnerability 10 months ago

M0rphling has been awarded the disclosure bounty   ✓

The fix bounty is now up for grabs

A **phoronix-test-suite/phoronix-test-suite** maintainer marked this as fixed in **10.8.0** with commit **5755b3** 10 months ago

The fix bounty has been dropped   ✗

This vulnerability will not receive a CVE   ✗

phoromatic_benchmark.php#L110 has been validated   ✓

Sign in to join this conversation

Chat with us

huntr

home

hacktivity

leaderboard

FAQ

contact us

terms

privacy policy

part of 418sec

company

about

team

Chat with us