Session Fixation in snipe/snipe-it

Valid Reported on Aug 22nd 2022

3

Description

The session is not invalidated after a password change.

Proof of Concept

Open Snipe-IT in the browser and login. Do the same in a private window such that there are two sessions. Change the password in one of the two sessions and observe that the second session is not invalidated.

Impact

An old session can be used even after the password has been changed.

References

- https://www.cobalt.io/vulnerability-wiki/v3-session-management/session-invalidate-failure-password-change

CVE
CVE-2022-2997
(Published)

Vulnerability Type
CWE-384: Session Fixation

Severity
Medium (4.6)

Registry
Other

Affected Version
6.0.9

Visibility
Public

Status
Fixed

Found by

vautia
@vautia
master

Fixed by

snipe
@snipe
maintainer

This report was seen 727 times.

We are processing your report and will contact the **snipe/snipe-it** team within 24 hours.
3 months ago

We have contacted a member of the **snipe/snipe-it** team and are waiting to hear back
3 months ago

snipe validated this vulnerability 3 months ago

vautia has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

snipe marked this as fixed in **6.0.10** with commit **6fde72** 3 months ago

snipe has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ✘

Sign in to join this conversation