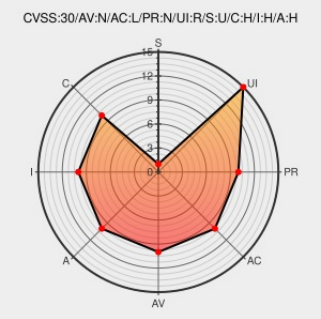
CVE-2019-5968

Published on: 07/05/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:00 PM UTC

CVE-2019-5968

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Growi from Weseek contain the following vulnerability:

Cross-site request forgery (CSRF) vulnerability in GROWI v3.4.6 and earlier allows remote attackers to hijack the authentication of administrators via updating user's 'Basic Info'.

CVE-2019-5968 has been assigned by vultures@jpcert.or.jp to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **WESEEK, Inc.** - **GROWI** version **v3.4.6 and earlier**

CVSS3 Score: 8.8 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	REQUIRED
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: 6.8 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
GROWI 脆弱性対応のお知らせ (JVN#84876282) | WESEEK, Inc.	Vendor Advisory, weseek.co.jp, text/html	MISC weseek.co.jp/security/2019/06/04/growi-fix-jvn84876282/

JVN#84876282: Multiple vulnerabilities in GROWI	Third Party Advisory jvn.jp text/xml	MISC jvn.jp/en/jp/JVN84876282/index.html

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Weseek	Growi	All	All	All	All

cpe:2.3:a:weseek:growi:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→