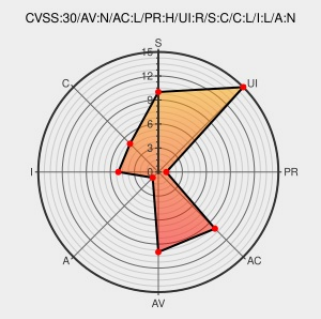
CVE-2018-0652

Published on: 09/07/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:48 PM UTC

CVE-2018-0652

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



Certain versions of Growi from Weseek contain the following vulnerability:

Cross-site scripting vulnerability in GROWI v.3.1.11 and earlier allows remote authenticated attackers to inject arbitrary web script or HTML via the UserGroup Management section of admin page.

CVE-2018-0652 has been assigned by vultures@jpcert.or.jp to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **WESEEK, Inc.** - **GROWI** version **v.3.1.11 and earlier**

CVSS3 Score: 4.8 - MEDIUM

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

CVSS2 Score: 3.5 - LOW

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

CVE References

Description	Tags	Link
GROWI 脆弱性対応のお知らせ (JVN#18716340) | WESEEK, Inc.	Vendor Advisory, weseek.co.jp, text/html	CONFIRM weseek.co.jp/security/2018/07/31/growi-prevent-xss/

JVN#18716340: Multiple cross-site scripting vulnerabilities in GROWI	Third Party Advisory VDB Entry jvn.jp text/xml	JVN JVN#18716340

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→