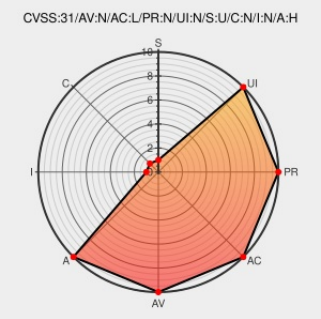
CVE-2020-5682

Published on: 12/16/2020 12:00:00 AM UTC

Last Modified on: 07/21/2021 11:39:00 AM UTC

CVE-2020-5682

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



Certain versions of Growi from Weseek contain the following vulnerability:

Improper input validation in GROWI versions prior to v4.2.3 (v4.2 Series), GROWI versions prior to v4.1.12 (v4.1 Series), and GROWI v3 series and earlier GROWI versions prior to v4.2.3 (v4.2 Series), GROWI versions prior to v4.1.12 (v4.1 Series), and GROWI v3 series and earlier allows remote attackers to cause a denial of service via unspecified vectors.

CVE-2020-5682 has been assigned by vultures@jpcert.or.jp to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **WESEEK, Inc.** - **GROWI** version **GROWI versions prior to v4.2.3 (v4.2 Series), GROWI versions prior to v4.1.12 (v4.1 Series), and GROWI v3 series and earlier**

CVSS3 Score: 7.5 - HIGH

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

CVSS2 Score: 5 - MEDIUM

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

CVE References

Description	Tags	Link

Description	Tags	Link
GitHub - weseek/growi: GROWI - Team collaboration software using markdown	Product Third Party Advisory github.com text/html	MISC github.com/weseek/growi
Docker Hub	Product Third Party Advisory hub.docker.com text/html	MISC hub.docker.com/r/weseek/growi/
JVN#94169589: Multiple vulnerabilities in GROWI	Third Party Advisory jvn.jp text/xml	MISC jvn.jp/en/jp/JVN94169589/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
Application	Weseek	Growi	All	All	All	All
Application	Weseek	Growi	All	All	All	All

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

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

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

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→