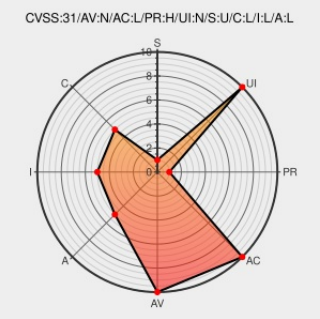
CVE-2021-20669

Published on: 03/10/2021 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:29:01 PM UTC

CVE-2021-20669

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



Certain versions of Growi from Weseek contain the following vulnerability:

Path traversal vulnerability in GROWI versions v4.2.2 and earlier allows an attacker with administrator rights to read and/or delete an arbitrary path via a specially crafted URL.

CVE-2021-20669 has been assigned by vultures@jpcert.or.jp to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **WESEEK, Inc.** - **GROWI** version **versions v4.2.2 and earlier**

CVSS3 Score: 4.7 - MEDIUM

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

CVSS2 Score: 6.5 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
JVNVU#94889258: Multiple vulnerabilities in GROWI	Third Party Advisory jvn.jp text/xml	MISC jvn.jp/en/vu/JVNVU94889258/index.html

GROWI 脆弱性対応のお知らせ (JVN#94889258) | WESEEK, Inc.	Vendor Advisory weseek.co.jp text/html	MISC weseek.co.jp/security/2021/03/08/vulnerability/growi-prevent-multiple-xss/

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→