CVE-2020-5676

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2020-5676
State	PUBLIC
Assigner	vultures@jpcert.or.jp
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-12-03 12:15:00 UTC
Updated	2020-12-03 14:54:00 UTC
Description	GROWI v4.1.3 and earlier allow remote attackers to obtain information which is not allowed to access via unspecified vecto

Risk And Classification

Problem Types: CWE-200

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference	Source	Link	Tags
GitHub - weseek/growi: GROWI - Team collaboration software using markdown	MISC	github.com	Product, Third Party Adviso
Docker Hub	MISC	hub.docker.com	Product, Third Party Adviso
JVN#56450373: Multiple vulnerabilities in GROWI	MISC	jvn.jp	Third Party Advisory
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report