



Published:2026/04/23 Last Updated:2026/04/23

JVN#46728373

GROWI vulnerable to Regular expression Denial-of-Service (ReDoS)

Overview

GROWI provided by GROWI, Inc. contains a Regular expression Denial-of-Service (DoS) vulnerability.

Products Affected

- GROWI v7.5.0 and earlier

Description

GROWI provided by GROWI, Inc. contains the following vulnerability.

- **Inefficient regular expression complexity (CWE-1333)**
 - CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N Base Score 8.7
 - CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H Base Score 7.5
 - CVE-2026-41040

Impact

An attacker may be able to cause a denial-of-service (DoS) attack.

Solution

Update the Software

Update the software to the latest version.

The developer has released the following version to address this vulnerability.

- GROWI v7.5.1 or later

For more details, refer to the information provided by the developer.

Vendor Status

| Vendor | Status | Last Update | Vendor Notes |
|--------------|----------------------------|-------------|--------------------------------------|
| WESEEK, Inc. | Vulnerable | 2026/04/23 | WESEEK, Inc. website |

References

JVN

| |
|--|
| HOME |
| What is JVN ? |
| Instructions |
| List of Vulnerability Report |
| VN_JP |
| VN_JP(Unreachable) |
| VN_VU |
| TA |
| TRnotes |
| JVN iPedia |
| MyJVN |
| JVNJS/RSS |
| Vendor List |
| List of unreachable developers |
| Contact |

JPCERT/CC Addendum

Vulnerability Analysis by JPCERT/CC

Credit

Sho Odagiri of GMO Cybersecurity by Ierae, Inc. reported this vulnerability to GROWI, Inc. and coordinated. After the coordination was completed, GROWI, Inc. reported the case to JPCERT/CC to notify users of the solution through JVN.

Other Information

JPCERT Alert

JPCERT Reports

CERT Advisory

CPNI Advisory

TRnotes

CVE [CVE-2026-41040](#)

JVN iPedia [JVND-2026-000064](#)

Copyright (c) 2000-2026 JPCERT/CC and IPA. All rights reserved.