

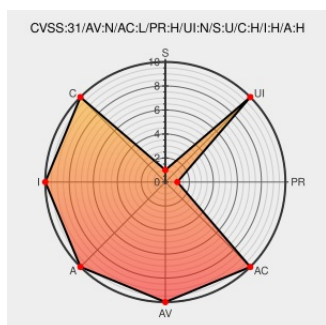


CVE-2020-10562

Published on: 03/13/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:34 PM UTC

CVE-2020-10562

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Grr](#) from [Devome](#) contain the following vulnerability:

An issue was discovered in DEVOME GRR before 3.4.1c.
admin_edit_room.php mishandles file uploads.

CVE-2020-10562 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **7.2 - HIGH**

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

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
sous-version 3.4.1c : mise à jour de sécurité · JeromeDevome/GRR@2c6edac · GitHub	Patch Third Party Advisory github.com text/html	MISC github.com/JeromeDevome/GRR/commit/2c6edacd9e15c75a0c2ef472470481ffb6ed

 [MISC github.com/skr0x/CVE/tree/master/CVE-2020-10562](https://github.com/skr0x/CVE/tree/master/CVE-2020-10562)

Release Notes
Third Party Advisory
github.com
text/html

comment@cve.report.

Known Affected Configurations (CPE V2.3)

```
cpe:2.3:a:devome:grr:*:*:*:*:*:
```

[← Previous ID](#)

Next ID→

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

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