

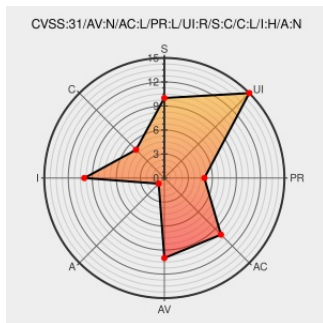


CVE-2020-5240

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

Last Modified on: 03/23/2021 11:24:03 PM UTC

CVE-2020-5240 - advisory for GHSA-9gjb-6qq6-v7qm

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

Certain versions of [Wagtail-2fa](#) from [Labdigital](#) contain the following vulnerability:

In wagtail-2fa before 1.4.1, any user with access to the CMS can view and delete other users 2FA devices by going to the correct path. The user does not require special permissions in order to do so. By deleting the other users device they can disable the target users 2FA devices and potentially compromise the account if they figure out their password. The problem has been patched in version 1.4.1.

CVE-2020-5240 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: Lab Digital - wagtail-2fa version < 1.4.1

CVSS3 Score: **8.5 - HIGH**

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

CVSS2 Score: **5.5 - MEDIUM**

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

CVE References

Description	Tags	Link
-------------	------	------

Prevent unauthorized users managing others' device · labd/wagtail-2fa@ac23550 · GitHub

Patch

Third Party Advisory

github.com

text/html

MISC

github.com/labd/wagtail-2fa/commit/ac23550d33b7436e90e3beea904647907eba5b74

2FA bypass through deleting devices · Advisory · labd/wagtail-2fa · GitHub

Third Party Advisory

github.com

text/html

CONFIRM

github.com/labd/wagtail-2fa/security/advisories/GHSA-9gjl-6qq6-v7qm

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

Related QID Numbers

983119 Python (pip) Security Update for wagtail-2fa (GHSA-9gjl-6qq6-v7qm)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Labdigital	Wagtail-2fa	All	All	All	All
Application	Labdigital	Wagtail-2fa	All	All	All	All
cpe:2.3:a:labdigital:wagtail-2fa:*****:						
cpe:2.3:a:labdigital:wagtail-2fa:*****:						

No vendor comments have been submitted for this CVE