



CVE-2021-31646

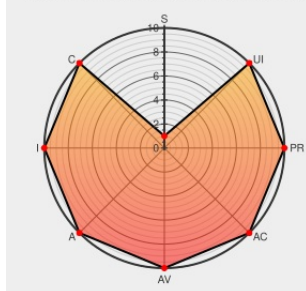
Published on: 04/26/2021 12:00:00 AM UTC

Last Modified on: 05/04/2021 12:32:00 AM UTC

CVE-2021-31646

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

CVSS:31/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H



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

Gestsup before 3.2.10 allows account takeover through the password recovery functionality (remote). The affected component is the file forgot_pwd.php - it uses a weak algorithm for the generation of password recovery tokens (the PHP uniqueid function), allowing a brute force attack.

CVE-2021-31646 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **CRITICAL** severity.

CVSS3 Score: **9.8 - CRITICAL**

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

CVSS2 Score: **7.5 - HIGH**

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

CVE References

Description	Tags	Link
GestSup Logiciel de gestion de support	gestsup.fr text/html	MISC gestsup.fr/index.php?page=download
GestSup Logiciel de gestion de	gestsup.fr	MISC: gestsup.fr/index.php?

gestsup | Login et gestion de support

gestsup
text/html

[misc gestsup/index.php?page=download&channel=beta&version=3.2.10&type=patch](#)

No Description Provided

dojo.maltem.ca
text/html

[MISC dojo.maltem.ca/public/advisories/CVE-2021-31646.html](#)

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.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Gestsup	Gestsup	All	All	All	All
cpe:2.3:a:gestsup:gestsup:*****:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-31646 : Gestsup before 3.2.10 allows account takeover through the password recovery functionality remote... twitter.com/i/web/status/1...	2021-04-26 18:42:47

← Previous ID

Next ID→