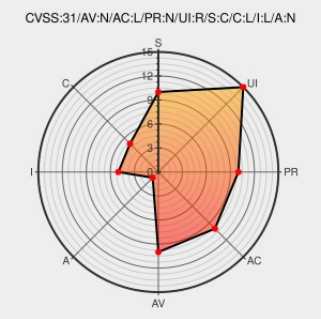
CVE-2021-31537

Published on: 05/11/2021 12:00:00 AM UTC

Last Modified on: 05/19/2021 08:22:00 PM UTC

CVE-2021-31537

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Sis-rewe Go from Sisinformatik contain the following vulnerability:

SIS SIS-REWE Go before 7.7 SP17 allows XSS: rewe/prod/web/index.php (affected parameters are config, version, win, db, pwd, and user) and /rewe/prod/web/rewe_go_check.php (version and all other parameters).

CVE-2021-31537 has been assigned by cve@mitre.org to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 6.1 - MEDIUM

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

CVSS2 Score: 4.3 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
Full Disclosure: SEC Consult SA-20210511-0 :: Cross-site Scripting Vulnerabilities in REWE GO	seclists.org text/html	MISC seclists.org/fulldisclosure/2021/May/20
SIS-REWE Go	sisinformatik.com text/html	MISC sisinformatik.com/rewe-go/

Reflected XSS Vulnerabilities in SIS Infromatik - Rewe Go	sec-consult.com text/html	MISC sec-consult.com/vulnerability-lab/advisory/reflected-xss-sis-infromatik-rewe-go-cve-2021-31537/
SIS-REWE GO 7.5.0/12C Cross Site Scripting ≈ Packet Storm	packetstormsecurity.com text/html	MISC packetstormsecurity.com/files/162530/SIS-REWE-GO-7.5.0-12C-Cross-Site-Scripting.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	Sisinformatik	Sis-rewe Go	All	All	All	All
Application	Sisinformatik	Sis-rewe Go	7.7	-	All	All
Application	Sisinformatik	Sis-rewe Go	7.7	sp16	All	All

cpe:2.3:a:sisinformatik:sis-rewe_go:*:*:*:*:*:*:*:*:

cpe:2.3:a:sisinformatik:sis-rewe_go:7.7:-:*:*:*:*:*:*:

cpe:2.3:a:sisinformatik:sis-rewe_go:7.7:sp16:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-31537 : SIS SIS-REWE Go before 7.7 SP17 allows #XSS: rewe/prod/web/index.php affected parameters are conf… twitter.com/i/web/status/1…	2021-05-11 15:07:25
/r/netcve	CVE-2021-31537	2021-05-11 15:41:42

← Previous ID

Next ID→

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