



Site Search



[Full Disclosure](#) mailing list archives



[By Date](#) [By Thread](#)

List Archive Search



SEC Consult SA-20210511-0 :: Cross-site Scripting Vulnerabilities in REWE GO

From: SEC Consult Vulnerability Lab <research () sec-consult com>

Date: Tue, 11 May 2021 08:36:19 +0200

SEC Consult Vulnerability Lab Security Advisory < 20210511-0 >
=====

title: Reflected Cross-site Scripting Vulnerabilities
product: SIS Informatik - REWE GO
vulnerable version: 7.5.0/12C
fixed version: 7.7 SP17
CVE number: CVE-2021-31537
impact: Medium
homepage: <https://sisinformatik.com/rewe-go/>
found: 2021-02-12
by: Steffen Robertz (Office Vienna)
Florian Lienhart (Office Vienna)
SEC Consult Vulnerability Lab

An integrated part of SEC Consult, an Atos company
Europe | Asia | North America

<https://www.sec-consult.com>

Vendor description:

"SIS Informatik is your specialist for the conception and implementation of tailor-made accounting, business intelligence and corporate performance management solutions. In addition to technical competence, business know-how and the willingness to develop optimal, adaptable software solutions together with our customers are the central components that make us a strong partner. We develop solutions based on high-quality technologies from well-known partners such as IBM, Oracle and Qlik" (translated from German)

Source: <https://sisinformatik.com/unternehmen/>

Business recommendation:

The vendor provides a patch which should be installed immediately.

SEC Consult recommends to perform a thorough security review of these products conducted by security professionals to identify and resolve all security issues.

Vulnerability overview/description:

1) Multiple Reflected Cross-site Scripting (XSS) (CVE-2021-31537)
The login website returns unfiltered or unescaped user input. This leads to a reflected cross-site scripting (XSS) vulnerability.
An attacker can inject arbitrary HTML or JavaScript code into the victim's web browser. Once the victim clicks on a malicious link, the attacker's code is executed in the context of the victim's web browser.

Proof of concept:

1) Multiple Reflected Cross-site Scripting (XSS) (CVE-2021-31537)
When opening the following URL the supplied JavaScript code will be executed.
/rewe/prod/web/index.php?config=rewe2&2&3E%3Cscript%3Ealert(%22document.domain%22)%3C/script%3E&version=7.5.0&win=2707&user=test&pwd=test&db=test&continue=false
The affected parameters are: "config", "version", "win", "db", "pwd", and "user".

No valid parameters need to be supplied to trigger the XSS vulnerability as seen in following URL:
/rewe/prod/web/index.php?abc'-alert(%22document.domain%22)='-abc=1

The following URL is affected as well:
/rewe/prod/web/rewe_go_check.php?config=rewe&version=7.5.0%3Cscript%3Ealert(1)%3C%2Fscript%3E&win=2707
All parameters are affected.

Vulnerable / tested versions:

The following product/firmware version has been tested:
* SIS-REWE GO 7.5.0/12C

Vendor contact timeline:

2021-02-24: Contacting vendor through office () sisworld com; no reply.
2021-03-11: Contacting vendor again through office () sisworld com.
2021-03-15: Vendor requests more information. SEC Consult offered to provide advisory via encrypted or unencrypted mail.
2021-03-17: Sending advisory via PGP encrypted mail.
2021-03-21: Vendor confirmed the vulnerability and is working on a patch.
2021-04-12: Requested status update.
2021-04-16: Hot fix 7.7 SP16 available in week 16, next release 7.7 SP17 in week 18.
2021-05-11: Coordinated release of security advisory.

Solution:

Contact the vendor in order to install the security patch for release 7.7 SP16 or upgrade to release 7.7 SP17. More information has been provided to customers of the vendor in a newsletter.

Workaround:

None

Advisory URL:

<https://sec-consult.com/vulnerability-lab/>

SEC Consult, an Atos company
Europe | Asia | North America

About SEC Consult Vulnerability Lab
The SEC Consult Vulnerability Lab is an integrated part of SEC Consult, an Atos company. It ensures the continued knowledge gain of SEC Consult in the field of network and application security to stay ahead of the attacker. The SEC Consult Vulnerability Lab supports high-quality penetration testing and the evaluation of new offensive and defensive technologies for our customers. Hence our customers obtain the most current information about vulnerabilities and valid recommendation about the risk profile of new technologies.

~~~~~  
Interested to work with the experts of SEC Consult?  
Send us your application <https://sec-consult.com/career/>

Interested in improving your cyber security with the experts of SEC Consult?  
Contact our local offices <https://sec-consult.com/contact/>  
~~~~~

Mail: research at sec-consult dot com
Web: <https://www.sec-consult.com>
Blog: <https://blog.sec-consult.com>
Twitter: https://twitter.com/sec_consult

EOF Steffen Robertz, Florian Lienhart / @2021


Attachment: [smime.p7s](#)
Description: S/MIME Cryptographic Signature





Sent through the Full Disclosure mailing list
<https://nmap.org/mailman/listinfo/fulldisclosure>
Web Archives & RSS: <http://seclists.org/fulldisclosure/>

[◀ By Date ▶](#) [◀ By Thread ▶](#)

Current thread:

SEC Consult SA-20210511-0 :: Cross-site Scripting Vulnerabilities in REWE GO SEC Consult Vulnerability Lab (May 10)



Nmap Security Scanner	Npcap packet capture	Security Lists	Security Tools	About	 
Ref Guide	User's Guide	Nmap Announce	Vuln scanners	About/Contact	
Install Guide	API docs	Nmap Dev	Password audit	Privacy	 
Docs	Download	Full Disclosure	Web scanners	Advertising	
Download	Npcap OEM	Open Source Security	Wireless	Nmap Public Source License	
Nmap OEM		BreachExchange	Exploitation		