SEC Consult SA-20220209 :: Open Redirect in Login Page in SIEMENS-SINEMA Remote Connect

From: "SEC Consult Vulnerability Lab, Research via Fulldisclosure" <fulldisclosure () seclists org>
Date: Wed, 9 Feb 2022 10:48:00 +0000

```
SEC Consult Vulnerability Lab Security Advisory < 20220209-0 >
=======================================================================
               title: Open Redirect in Login Page
             product: SIEMENS-SINEMA Remote Connect
  vulnerable version: V1.0 SP3 HF1
       fixed version: V2.0 has been out since April, 2019
          CVE number: CVE-2022-23102
              impact: Low
            homepage: https://www.siemens.com
               found: 2021-11-18
                  by: A. Ovsyannikova (Office Moscow)
                      SEC Consult Vulnerability Lab

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

                      https://www.sec-consult.com

=======================================================================

Vendor description:
-------------------
"Siemens is a technology company focused on industry, infrastructure, transport, and
healthcare.
 From more resource-efficient factories, resilient supply chains, and smarter buildings and
grids,
to cleaner and more comfortable transportation as well as advanced healthcare, we create
technology with purpose adding real value for customers. By combining the real and the
digital
worlds, we empower our customers to transform their industries and markets, helping them
to transform the everyday for billions of people."

Source: https://www.siemens.com


Business recommendation:
------------------------
The vendor provides a patched version for the affected product since April 2019, but the
security notes have been published now.
```

An in-depth security analysis performed by security professionals is highly advised, as the software may be affected from further security issues.

Vulnerability overview/description:
---
1) Open Redirect in Login Page (CVE-2022-23102)
An open redirect vulnerability can be triggered by luring a user to authenticate to a SIEMENS-SINEMA Remote Connect device by clicking on a crafted link.
By abusing this vulnerability, an attacker could steal logon credentials with a specially crafted phishing page or exploit browser vulnerabilities.

Proof of concept:
---
1) Open Redirect in Login Page (CVE-2022-23102)
After a successful login of the victim, the user will be redirected to https://www.sec-consult.com
when the following link is being clicked:

https://$IP/wbm/login/?next=https://www.sec-consult.com

Vulnerable / tested versions:

The following version has been tested and found to be vulnerable:
* SIEMENS-SINEMA Remote Connect Client V1.0 SP3 HF1

Vendor contact timeline:

2021-12-13: Contacting CERT through cert () siemens com and requested support for the disclosure process.
2021-12-15: Siemens opened case #32494 to track this issue.
2022-01-12: Security contact informed us, that some vulnerabilities were fixed by the vendor back in 2019 but they will issue a CVE and an advisory for 8th Feb 2022.
2022-01-18: Siemens has reserved the CVE number CVE-2022-23102.
2022-02-08: Release of Siemens advisory CVE-2022-23102.
2022-02-09: Release of security advisory.

Solution:

The vendor provides a patched version V2.0 for the affected product since April 2019, but the
security notes have been published now at:

https://cert-portal.siemens.com/productcert/pdf/ssa-654775.pdf

Workaround:

None

Advisory URL:
---
https://sec-consult.com/vulnerability-lab/

~~~~~~

SEC Consult 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: http://blog.sec-consult.com
Twitter: https://twitter.com/sec_consult

EOF A.Ovsyannikova / @2022

By Date By Thread

Current thread:

SEC Consult SA-20220209 :: Open Redirect in Login Page in SIEMENS-SINEMA Remote Connect
SEC Consult Vulnerability Lab, Research via Fulldisclosure (Feb 10)

Site Search

Nmap Security Scanner
Ref Guide
Install Guide
Docs
Download
Nmap OEM

Npcap packet capture
User's Guide
API docs
Download
Npcap OEM

Security Lists
Nmap Announce
Nmap Dev
Full Disclosure
Open Source Security
BreachExchange

Security Tools
Vuln scanners
Password audit
Web scanners
Wireless
Exploitation

About
About/Contact
Privacy
Advertising
Nmap Public Source License