SIEMENS-SINEMA Remote Connect 1.0 SP3 HF1 Open Redirection

Authored by A. Ovsyannikova | Site sec-consult.com

Posted Feb 11, 2022

SIEMENS-SINEMA Remote Connect version 1.0 SP3 HF1 suffers from an open redirection vulnerability.

tags | exploit, remote
advisories | CVE-2022-23102
SHA-256 | 2025fbf79c79ed214e16d6403fd3fd60fe1acdc9c72cd918baa2eba0b4448e75 **Download** | **Favorite** | **View**

Related Files

Change Mirror Download

```
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.
```


File Archive: November 2022 <

Su	Mo	Tu	We	Th	Fr	Sa
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30			

Top Authors In Last 30 Days

Red Hat 186 files
Ubuntu 52 files
Gentoo 44 files
Debian 27 files
Apple 25 files
Google Security Research 14 files
malvuln 10 files
nu11secur1ty 6 files
mjurczyk 4 files
George Tsimpidas 3 files

File Tags

ActiveX (932)
Advisory (79,557)
Arbitrary (15,643)
BBS (2,859)
Bypass (1,615)
CGI (1,015)
Code Execution (6,913)
Conference (672)
Cracker (840)
CSRF (3,288)
DoS (22,541)
Encryption (2,349)
Exploit (50,293)
File Inclusion (4,162)
File Upload (946)
Firewall (821)
Info Disclosure (2,656)

File Archives

November 2022
October 2022
September 2022
August 2022
July 2022
June 2022
May 2022
April 2022
March 2022
February 2022
January 2022
December 2021
Older

Systems

AIX (426)
Apple (1,926)

```
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
```


Intrusion Detection (866)
Java (2,888)
JavaScript (817)
Kernel (6,255)
Local (14,173)
Magazine (586)
Overflow (12,390)
Perl (1,417)
PHP (5,087)
Proof of Concept (2,290)
Protocol (3,426)
Python (1,449)
Remote (30,009)
Root (3,496)
Ruby (594)
Scanner (1,631)
Security Tool (7,768)
Shell (3,098)
Shellcode (1,204)
Sniffer (885)
Spoof (2,165)
SQL Injection (16,089)
TCP (2,377)
Trojan (685)
UDP (875)
Virus (661)
Vulnerability (31,104)
Web (9,329)
Whitepaper (3,728)
x86 (946)
XSS (17,478)
Other

BSD (370)
CentOS (55)
Cisco (1,917)
Debian (6,620)
Fedora (1,690)
FreeBSD (1,242)
Gentoo (4,272)
HPUX (878)
iOS (330)
iPhone (108)
IRIX (220)
Juniper (67)
Linux (44,118)
Mac OS X (684)
Mandriva (3,105)
NetBSD (255)
OpenBSD (479)
RedHat (12,339)
Slackware (941)
Solaris (1,607)
SUSE (1,444)
Ubuntu (8,147)
UNIX (9,150)
UnixWare (185)
Windows (6,504)
Other

Site Links

News by Month
News Tags
Files by Month
File Tags
File Directory

About Us

History & Purpose
Contact Information
Terms of Service
Privacy Statement
Copyright Information

Hosting By

Rokasec

Follow us on Twitter
Subscribe to an RSS Feed