CODESYS 2.4.7.0 Denial Of Service

Authored by Gerhard Hechenberger, Steffen Robertz | Site sec-consult.com

Posted Nov 1, 2021

CODESYS Runtime Toolkit 32-bit versions prior to 2.4.7.56 suffer from a denial of service vulnerability.

tags | advisory, denial of service
advisories | CVE-2021-34593
SHA-256 | e2c08ed088508dee09719da1812fdba8c069873d79d63fec42f1375ec7b871d9 **Download** | **Favorite** | **View**

Related Files

Share This

Like Twee LinkedIn Reddit Digg StumbleUpon

Change Mirror Download

```
SEC Consult Vulnerability Lab Security Advisory < 20211028-0 >
=======================================================================
              title: CODESYS V2 Denial of Service
            product: CODESYS Runtime Toolkit 32-bit, CODESYS PLCWinNT
 vulnerable version: <V2.4.7.56
      fixed version: V2.4.7.56
         CVE number: CVE-2021-34593
             impact: High
           homepage: https://www.codesys.com/
              found: 2021-05-05
                 by: SEC Consult Vulnerability Lab
                     This vulnerability was discovered during the research
                     cooperation initiative "OT Cyber Security Lab" between
                     Verbund AG and SEC Consult Group.
                     Gerhard Hechenberger (Office Vienna)
                     Steffen Robertz (Office Vienna)

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

                     https://www.sec-consult.com

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

Vendor description:
-------------------
"CODESYS is the leading manufacturer-independent IEC 61131-3 automation
software for engineering control systems."

Source: https://www.codesys.com/


Business recommendation:
------------------------
The vendor provides patches. The vendors of products using the affected
software should provide new firmware versions immediately. Users of these
products should update their devices to those fixed firmware versions.


Vulnerability overview/description:
-----------------------------------
The CODESYS Control runtime system is the core of many PLCs. The runtime is
accepting TCP connections on a pre-configured port to connect to the
development system. By sending requests that define an invalid packet size,
a memory allocation error can be triggered. This leads to a denial of service
condition of the remote connectivity of the CODESYS service, which prevents
clients from connecting to the affected PLC.

CODESYS released a dedicated security note, which corresponds to this advisory:
https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=16877&token=8faab0fc1e069f4edfca5d5aba8146139f67a175


Proof of concept:
-----------------
A detailed proof of concept will be made public after the affected product
vendors had time to provide new firmware versions.


Vulnerable / tested versions:
-----------------------------
2.4.7.0


Vendor contact timeline:
------------------------
2021-05-25: Contacting 3rd party vendor of a product using the CODESYS runtime
            about this issue.
2021-08-11: Vendor states that this issue was already fixed in a recent CODESYS
            release.
2021-08-18: A check on the product's most recent public firmware release
            shows that the vulnerability still exists. The vendor is notified
            again about this outcome.
2021-09-01: The vendor confirms and ensures the issue is investigated in
            collaboration with CODESYS.
2021-10-15: CODESYS informs about the assigned CVE-2021-34593 and the planned
            publishing date.
2021-10-28: Coordinated release.


Solution:
---------
Immediately update to the patched version of CODESYS.


Workaround:
-----------
To mitigate this issue, access to the CODESYS service port of the affected
devices should be limited as far as possible. In the long run, the updated
firmware of the product vendor containing a patched CODESYS service must be
installed.


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
```

Follow us on Twitter

Subscribe to an RSS Feed

File Archive: December 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	31

Top Authors In Last 30 Days

Red Hat	157 files
Ubuntu	76 files
LiquidWorm	23 files
Debian	21 files
nu11secur1ty	11 files
malvuln	11 files
Gentoo	9 files
Google Security Research	8 files
Julien Ahrens	4 files
T. Weber	4 files

File Tags

ActiveX	(932)
Advisory	(79,754)
Arbitrary	(15,694)
BBS	(2,859)
Bypass	(1,619)
CGI	(1,018)
Code Execution	(6,926)
Conference	(673)
Cracker	(840)
CSRF	(3,290)
DoS	(22,602)
Encryption	(2,349)
Exploit	(50,359)
File Inclusion	(4,165)
File Upload	(946)
Firewall	(821)
Info Disclosure	(2,660)
Intrusion Detection	(867)
Java	(2,899)
JavaScript	(821)
Kernel	(6,291)
Local	(14,201)
Magazine	(586)
Overflow	(12,419)
Perl	(1,418)
PHP	(5,093)
Proof of Concept	(2,291)
Protocol	(3,435)
Python	(1,467)
Remote	(30,044)
Root	(3,504)
Ruby	(594)
Scanner	(1,631)
Security Tool	(7,777)
Shell	(3,103)
Shellcode	(1,204)
Sniffer	(886)

File Archives

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

Systems

AIX	(426)
Apple	(1,926)
BSD	(370)
CentOS	(55)
Cisco	(1,917)
Debian	(6,634)
Fedora	(1,690)
FreeBSD	(1,242)
Gentoo	(4,272)
HPUX	(878)
iOS	(330)
iPhone	(108)
IRIX	(220)
Juniper	(67)
Linux	(44,315)
Mac OS X	(684)
Mandriva	(3,105)
NetBSD	(255)
OpenBSD	(479)
RedHat	(12,469)
Slackware	(941)
Solaris	(1,607)

```
Blog: http://blog.sec-consult.com
Twitter: https://twitter.com/sec_consult

EOF Gerhard Hechenberger, Steffen Robertz / @2021
```

Login or Register to add favorites

- Spoof (2,166)
- SQL Injection (16,102)
- TCP (2,379)
- Trojan (686)
- UDP (876)
- Virus (662)
- Vulnerability (31,136)
- Web (9,365)
- Whitepaper (3,729)
- x86 (946)
- XSS (17,494)
- Other

- SUSE (1,444)
- Ubuntu (8,199)
- UNIX (9,159)
- UnixWare (185)
- Windows (6,511)
- 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

packet storm