WAGO 750-8xxx PLC Denial Of Service / User Enumeration

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

Posted Feb 4, 2022

WAGO 750-8xxx PLC versions prior to Firmware 20 Patch 1 (v03.08.08) suffer from denial of service and user enumeration vulnerabilities.

tags | exploit, denial of service, vulnerability
advisories | CVE-2021-34593
SHA-256 | 3baa93a2d3f1b5ab0f4e0408fec68f1c11444bf8af50dc66f28f63e877786d44 Download | Favorite | View

Related Files

Change Mirror Download

```
SEC Consult Vulnerability Lab Security Advisory < 20220126-0 >
=======================================================================
               title: Denial of service & User Enumeration
             product: WAGO 750-8xxx PLC
  vulnerable version: < Firmware 20 Patch 1 (v03.08.08)
       fixed version: Firmware 20 Patch 1 (v03.08.08)
          CVE number: CVE-2021-34593
              impact: Medium
            homepage: https://www.wago.com/
               found: 2021-05-05
                  by: SEC Consult Vulnerability Lab
                      These vulnerabilities were 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:
-------------------
"Optimum performance and availability: Thanks to their ultra-high performance,
low power consumption, numerous interfaces, space-saving design and high
reliability, WAGO's user-friendly controllers (PLCs) are cost-effective
automation solutions. For optimal automation both inside and outside the
control cabinet: the flexible IP20 remote I/O systems for all applications
and environments."

Source: https://www.wago.com/us/c/controllers-bus-couplers-i-o


Business recommendation:
------------------------
WAGO's customers should upgrade the firmware to the latest version available.

A thorough security review should be performed by security professionals to
identify further security issues.


Vulnerability overview/description:
-----------------------------------
1) Denial of Service (Codesys) (CVE-2021-34593)
The "plclinux_rt" binary is listening on port 2455. It handles communication with
the CODESYS suite. By sending requests that define an invalid packet size, a
malloc error can be triggered. This leads to a denial of service of the remote
connectivity of the codesys service.

This was also reported to and released together with CODESYS, find the
corresponding advisories here:
https://sec-consult.com/vulnerability-lab/advisory/codesys-v2-denial-of-service/
https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=16877&token=8faab0fc1e069f4edfca5d5aba8146139f67a175


2) Enumeration of Users
Due to a time-based side channel vulnerability, it can be derived which
usernames are valid. This eases the process of brute-forcing valid credentials.


3) Outdated Software with Known Vulnerabilities
The PLC is using multiple outdated software components with known exploits.


4) Insufficient Hardening of Binaries
Multiple binaries are not compiled with available security features. This will
ease further attacks once a memory corruption vulnerability has been spotted.


Proof of concept:
-----------------
1) Denial of Service (Codesys) (CVE-2021-34593)
Codesys packet headers are structured like below (pseudo code):

struct codesys_header {
    uint16_t magic,
    int32_t packet_size
}

The magic bytes will be 0xbbbb. By defining a packet size of 0xffffffff, a size
of 4 GB is defined. The following pseudo code will be used to handle the
request:

allocated_mem = (byte*)SysAllocDataMemory(coedesys_header.packet_size);
buffer_info->recv_buf_wout_header = allocated_mem;
if (allocated_mem == (byte *)0x0) {
     return;
}

As 4GB of memory aren't available, malloc will return a NULL pointer, which is
passed back through the SysAllocDataMemory() function and the return statement
in the pseudo code will be hit. Thus, the TCPServerTask() function will return.
The file descriptor for the client is not cleared in advance. Therefore, the
socket stays open indefinitely. A new client will open the next file
descriptor. As only 19 clients are allowed to be connected simultaneously, it
is sufficient to send 19 requests with a wrong packet length to force the PLC
into a state where it will refuse further connections to the Codesys service.

The current implementation is missing the call to SysSockClose() once a buffer
allocation fails.


2) Enumeration of Users
A time-based side channel vulnerability in the webserver's authentication
method is leaking information about valid usernames. The following code snippet is
used in the login method:

// get password file and iterate over every line
$pwFileArray = file($passwordFilename);
foreach($pwFileArray as $lineNo => $pwFileLine)
{
   // extract username and user password
   $passwordFileData = explode(':', trim($pwFileLine));
   // if username was found in line, verify given password with user password
   if(isset($passwordFileData[0]) && ($passwordFileData[0] === $username))
   {
     $pwCorrect = password_verify($password, $passwordFileData[1]);
     break;
   }
```


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)

}

The password hash is only calculated if the username is found to be valid. As the PLC has limited computational power, this results in different timings for the response depending on the validity of the username. The following script can be used to find valid users. The parameter 'delay_valid' might need to be adjusted to the network speed:

```
---------------------------
#!/usr/sbin/python
import requests
import sys
import urllib3
urllib3.disable_warnings(urllib3.exceptions.InsecureRequestWarning)

delay_valid = 0.2

f = open(sys.argv[1],"r");

for user in f.readlines():
     payload =
{"username":user.replace('\n',''),"password":"AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     cnt = 0
     for i in range(5):
         try:
             r = requests.post("https://<your_PLC_IP>/wbm/php/authentication/login.php", json=payload,
timeout=delay_valid, verify=False)
         except:
             cnt = cnt +1
     if cnt >=3:
         print("[*]Valid User: {}".format(user))
----------------------------
```

3) Outdated Software with Known Vulnerabilities
Following outdated and vulnerable components were identified by using the IoT Inspector firmware analysis tool:

- Dsnmasq 2.80: 9 CVEs
- Bash 4.4.23: 1 CVE
- GNU glibc 2.30: 12 CVEs
- Linux Kernel 4.9.146: 663 CVEs
- OpenSSL 1.0.1: 103 CVEs
- BusyBox 1.30.1: 2 CVEs
- Curl 7.72.0: 1 CVE
- OpenSSH 7.9p1: 4 CVEs
- PHP 7.3.15: 11 CVEs
- Wpa_supplicant 2.6: 20 CVEs
- NET-SNMP 5.8: 1 CVE
- Libpcap 1.8.1: 5 CVEs
- Info-ZIP 3.0: 13 CVEs

4) Insufficient Hardening of Binaries
The following features were extracted with the IoT Inspector:
- 1.9% of all executables support full RELRO
- 84.6% support partial RELRO
- Only 3.6% of all executables make use of stack canaries
- 58.9% are using ASLR/PIE

The plclinux_rt binary is an example of a particularly vulnerable binary. It accepts user input on port 2455 and is missing all compile-time security features. Thus, it's a perfect candidate to successfully exploit any identified buffer overflow.

Vulnerable / tested versions:

The following versions have been tested and found to be vulnerable:
* WAGO 750-8xxx Firmware 18 (v03.06.11)
* WAGO 750-8xxx Firmware 15 (v03.03.10)

Vendor contact timeline:

2021-05-25: Contacting vendor through support.at@wago.com, asking for security contact information. Support informed about their PSIRT team. Set preliminary release date to 2021-07-14.
2021-05-26: Contacting PSIRT through psirt@wago.com for encryption options.
2021-05-27: Received PGP key from PSIRT, transmitted encrypted advisory to psirt@wago.com.
2021-05-31: Wago PSIRT notifies about decryption problems.
2021-06-02: Wago PSIRT redirects to VDE CERT for encrypted transmission. Transmitted encrypted advisory to info@cert.vde.com. Set release date to 2021-07-22. Wago PSIRT resolves decryption problems.
2021-06-07: Received confirmation from VDE CERT.
2021-08-11: On request, Wago PSIRT informs about the investigation results and mentions that the DoS was already reported and is fixed with firmware 18 patch 3.
2021-08-18: A check on the most recent public firmware release v18 (v03.06.19) shows that the vulnerability still exists. Wago PSIRT is notified.
2021-09-01: Wago PSIRT confirms and ensures the issue is investigated.
2021-09-29: Request status from Wago PSIRT. Set new release date to 2021-11-16.
2021-09-30: Wago PSIRT states that CODESYS provided a fix which is currently tested and to wait for a coordinated release with CODESYS.
2021-10-15: CODESYS informs about the assigned CVE-2021-34593 and the planned publishing date.
2021-10-18: Requesting information from Wago on an updated firmware version.
2021-10-19: Wago PSIRT states that they just received the new CODESYS sources and it will take some more weeks to create a new firmware release.
2021-10-28: CODESYS vulnerability CVE-2021-34593 is released in a coordinated manner together with CODESYS group without exploit details.
2021-11-30: Request status from Wago PSIRT on new firmware release.
2022-01-17: Request status from Wago PSIRT on new firmware release again.
2022-01-18: Wago PSIRT informs that firmware 20 Patch 1 released on January 10, 2022 fixes the remaining issue. The firmware was not yet published on their website.
2022-01-26: Release of security advisory.

Solution:

Immediately update the PLCs to the fixed firmware version provided by the vendor to mitigate CVE-2021-34593.

The fixed firmware release 20 patch 1 can be obtained from
https://www.wago.com/de/d/6599873

Regarding vulnerability 2)
As stated by Wago, there are only two possible default usernames. Therefore, the username enumeration may not gain additional information and this will not be changed.

Additionally, due to varying release cycles, there is a delay in updating components (affecting the other identified vulnerabilities). It is planned to change to a new distribution release with firmware 20.

Workaround:

None

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

```
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
```


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

```
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 Gerhard Hechenberger, Steffen Robertz / @2022
```