



Site Search

[Full Disclosure](#) mailing list archives[By Date](#) [By Thread](#)

List Archive Search



SEC Consult SA-20220531-0 :: Backdoor account in Korenix JetPort 5601V3

From: "SEC Consult Vulnerability Lab, Research via Fulldisclosure" <fulldisclosure () seclists.org>

Date: Tue, 31 May 2022 10:13:02 +0000

SEC Consult Vulnerability Lab Security Advisory < 20220531-0 >

```
=====
                title: Backdoor account
                product: Korenix JetPort 5601V3
vulnerable version: Firmware version 1.0
                fixed version: None
                CVE number: CVE-2020-12501
                impact: High
                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 [...].

Our products are mainly applied in SMART industries: Surveillance, Machine-to-Machine, Automation, Remote Monitoring, and Transportation. 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 stated that they "will not remove the hardcoded backdoor account as it is needed for customer support and it can't be cracked in a reasonable amount of time."

SEC Consult recommends not to use those devices in production environments and to perform a thorough security review conducted by security professionals to identify and resolve potential further critical security issues.

Vulnerability overview/description:

1) 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. A telnet service is running on the device by default. This increases the risk of exploitation on the local network.

Proof of concept:

1) Backdoor Accounts (CVE-2020-12501)
The following account is available on at least one JetPort device of Korenix. There might be more affected devices across this vendor. Westerno and Control devices may be affected too.

```
* User "superrd", present on:
- JetPort 5601V3
  More devices may be affected.
```

Two other users are present on the system according to "/etc/passwd". An additional telnet-daemon is listening on port 19999.

```
root:<no password>
superrd:<not cracked>
admin:admin
```

By inspecting "/etc/passwd", the only user that is allowed to login to the device is "superrd":

```
root::0:0:root:/root:/bin/false
superrd:$1$<redacted>:0:0::/root:/bin/sh
admin:$1$$CoERg7ynjYLSj2j4g1J34.:502:502:::/bin/true
```

The listener has been identified by using "ps" and "netcat":

```
# ps
  PID  Uid      VmSize  Stat Command
    1  root      1452 S    init [3]
[...]
```

PID	Uid	VmSize	Stat	Command
253	root	1780	S	/usr/bin/ser2net -p 600 -c /tmp/com2ip.conf
254	root	288	S	/usr/sbin/telnetd -p 19999
289	root	788	S	/usr/bin/dropbear
297	root	1916	S	/usr/bin/thttpd -C /etc/thttpd.conf -cert /etc/thttpd

```
# netstat -tuln
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
[...]
```

Proto	Recv-Q	Send-Q	Local Address	Foreign Address	State
tcp	0	0	0.0.0.0:19999	0.0.0.0:*	LISTEN

```
[...]
```

The vulnerability has been manually verified on an emulated device by using the MEDUSA scalable firmware runtime.

Vulnerable / tested versions:

The following product / firmware version has been tested:
* Korenix JetPort 5601V3 / 1.0

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 () beijeirelectronics.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 () beijeirelectronics.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 () beijeirelectronics.com. Received confirmation of advisory receipt. Security manager told us that he can provide information regarding the timeline 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.

2021-06-24: Beijer Electronics contact informs us that he leaves the company today. Refers us to new contact in CC.

2021-07-05: Follow-up meeting with new vendor contact 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 2021. 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: Released related advisory SA-20220131-0.

2022-02-22: Vendor says, that fixes are estimated to be completed by end of February.

2022-03-29: Most issues from the related advisories (SA-20201005-0, SA-20210601-0) are not applicable according to the vendor, only the backdoor account exists in the JetPort series. The JetPort series will not go end of life.

The backdoor is needed in order to assist customers with problems and Korenix claims the password can't be cracked in a reasonable amount of time, hence it will not be fixed.

Security contact states that there is no point in waiting and we can release the security advisory.

2022-04-05: Another call to clarify with security contact; Korenix will not remove the account as this issue is not considered as critical.

2022-05-18: Tried to re-send the advisory for final review which only contains the backdoor account information. Received auto-reply that our contact from Beijer Group (who did the coordination with Korenix) was no longer part of the company.

2022-05-31: Public release of security advisory.

Solution:

None available. The vendor stated that they "will not remove the hardcoded backdoor account as it is needed for customer support and it can't be cracked in a reasonable amount of time."

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: security-research at sec-consult dot com

Web: <https://www.sec-consult.com>

Blog: <http://blog.sec-consult.com>





Twitter: https://twitter.com/sec_consult

[By Date](#) [By Thread](#)

Current thread:

SEC Consult SA-20220531-0 :: Backdoor account in Korenix JetPort 5601V3 SEC Consult Vulnerability Lab, Research via Fulldisclosure (Jun 03)

Site Search

Nmap Security Scanner	Npcap packet capture	Security Lists	Security Tools	About	 
Ref Guide	User's Guide	Nmap Announce	Vuln scanners	About/Contact	
Install Guide	API docs	Nmap Dev	Password audit	Privacy	 
Docs	Download	Full Disclosure	Web scanners	Advertising	
Download	Npcap OEM	Open Source Security	Wireless	Nmap Public Source License	
Nmap OEM		BreachExchange	Exploitation		