

- [Risk Management](#)
- [Compliance](#)
- [Privacy](#)
- [Supply Chain](#)
- ▼ [Security Architecture](#)
 - [Cloud Security](#)
 - [Identity & Access](#)
 - [Data Protection](#)
 - [Network Security](#)
 - [Application Security](#)
- ▼ [Security Strategy](#)
 - [Risk Management](#)
 - [Security Architecture](#)
 - [Disaster Recovery](#)
 - [Training & Certification](#)
 - [Incident Response](#)
- [ICS/OT](#)
- [IoT Security](#)

[Home](#) > [ICS/OT](#)



Vendor Refuses to Remove Backdoor Account That Can Facilitate Attacks on Industrial Firms

By [Eduard Kovacs](#) on June 01, 2022

Share

Tweet

推荐 0



Korenix JetPort industrial serial device servers have a backdoor account that could be abused by malicious hackers in attacks aimed at industrial organizations, but the vendor says the account is needed for customer support.

The [existence of the backdoor account](#), tracked as CVE-2020-12501, was discovered by Austria-based cybersecurity consultancy SEC Consult in 2020, but it was only made public now, after a lengthy disclosure process that ended with the vendor saying that the account will not be removed.

The account in question can be exploited by an attacker on the network to access the device's operating system and gain full control. The attacker could reconfigure the device and possibly gain access to other systems attached to the server.

The issue was identified in the Korenix JetPort 5601V3 product, which is designed for connectivity in industrial environments. SEC Consult believes other products — including Westermo and Control branded industrial devices — may also be impacted.

Beijer Electronics, the parent company of industrial networking solutions provider Korenix, has been contacted for comment.

SEC Consult told *SecurityWeek* that the backdoor account has the same password on all devices as it's stored in the firmware. Once an attacker has cracked the password — the password is not stored in clear text and needs to be cracked — it can be used to attack all affected devices. Moreover, the password cannot be changed by the user.

The vendor told SEC Consult the backdoor account is needed for customer support and argued that the password “can't be cracked in a reasonable amount of time.”

SEC Consult admitted that it could not immediately crack the password, but it has not put too much effort into the task. The password hash has not been made public, but it can easily be extracted from the firmware.

The company says there are better solutions for helpdesk access, ones that don't require the use of backdoors.

This is not the first time a researcher has found hardcoded credentials in JetPort devices. Back in 2012, ICS-CERT [warned organizations](#) about credentials that could have been abused for admin access, but that vulnerability was at some point patched with a firmware update.

Related: [Industrial Switches From Several Vendors Affected by Same Vulnerabilities](#)

Related: [Vulnerabilities Can Allow Hackers to Create Backdoors in Control Industrial Gateways](#)

[Share](#)[Tweet](#)[推荐 0](#)[RSS](#)

Eduard Kovacs ([@EduardKovacs](#)) is a contributing editor at SecurityWeek. He worked as a high school IT teacher for two years before starting a career in journalism as Softpedia's security news reporter. Eduard holds a bachelor's degree in industrial informatics and a master's degree in computer techniques applied in electrical engineering.

Previous Columns by Eduard Kovacs:

[Millions of Budget Smartphones With UNISOC Chips Vulnerable to Remote DoS Attacks](#)

[Leaks Show Conti Ransomware Group Working on Firmware Exploits](#)

[Coralogix Raises \\$142 Million for Data Observability Platform](#)

[Unpatched Vulnerability Exposes Horde Webmail Servers to Attacks](#)

[Ransomware Group Claims to Have Breached Foxconn Factory](#)

[Virtual Event Series - Security Summit Online Events by SecurityWeek](#)

sponsored links

[2022 ICS Cyber Security Conference | USA \[Hybrid: Oct. 24-27\]](#)

[2022 Singapore/APAC ICS Cyber Security Conference](#)

[2022 CISO Forum: September 13-14 - A Virtual Event](#)

 **Tags:**

[ICS/OT](#) [NEWS & INDUSTRY](#) [Vulnerabilities](#)