Schneider Electric Security Notification

NTZ Mekhanotronika Rus. LLC SHFK-MT-104 Control Panels

10 August 2021

Overview

Schneider Electric is aware of multiple Microsoft Windows® vulnerabilities in its NTZ Mekhanotronika Rus. LLC SHFK-MT-104 control panels.

NTZ Mekhanotronika Rus. LLC offers that contain Microsoft Windows® operating system as part of the products could be affected by the vulnerabilities listed below. An attacker may be able to take control of the system through the exploitation of the vulnerabilities. All impacted customers are requested to follow the recommendations in this document to eliminate the possibility of such an attack.

Affected Products and Versions

Affected Product	Serial Number	Microsoft Windows® version
SHFK-MT-104 DIVG.424327.104-35	3203	MICROSOFT WIN 10 PRO, P/N: FQC-08909-D
SHFK-MT-104 DIVG.424327.104-41	3520	MICROSOFT WIN 10 PRO, P/N: FQC-08909-D
SHFK-MT-104 DIVG.424327.104-36.01 SHFK-MT-104 DIVG.424327.104-36.20	3297 - 3316	MICROSOFT WIN 10 PRO Version 1909, P/N: FQC-08909-D
SHFK-MT-104 DIVG.424327.104-36.21 SHFK-MT-104 DIVG.424327.104-36.25	3368 - 3372	MICROSOFT WIN 10 PRO Version 1909, P/N: FQC-08909-D
SHFK-MT-104 DIVG.424327.104-36.26 SHFK-MT-104 DIVG.424327.104-36.65	3318 - 3357	MICROSOFT WIN 10 PRO Version 1909, P/N: FQC-08909-D
SHFK-MT-104 DIVG.424327.104-36.66 SHFK-MT-104 DIVG.424327.104-36.70	3505 - 3509	MICROSOFT WIN 10 PRO Version 1909, P/N: FQC-08909-D
SHFK-MT-104 DIVG.424327.104-36.71 SHFK-MT-104 DIVG.424327.104-36.80	3373 - 3382	MICROSOFT WIN 10 PRO Version 1909, P/N: FQC-08909-D
SHFK-MT-104 DIVG.424327.104-36.81 SHFK-MT-104 DIVG.424327.104-37.11	3394 - 3423	MICROSOFT WIN 10 PRO Version 1909, P/N: FQC-08909-D
SHFK-MT-104 DIVG.424327.104-37.12 SHFK-MT-104 DIVG.424327.104-37.21	3510 - 3519	MICROSOFT WIN 10 PRO Version 1909, P/N: FQC-08909-D
SHFK-MT-104 DIVG.424327.104-37.22 SHFK-MT-104 DIVG.424327.104-37.81	3552 - 3611	MICROSOFT WIN 10 PRO Version 1909, P/N: FQC-08909-D
SHFK-MT-104 DIVG.424327.104-37.82 SHFK-MT-104 DIVG.424327.104-38.01	3697 - 3715	MICROSOFT WIN 10 PRO Version 1909, P/N: FQC-08909-D
SHFK-MT-104 DIVG.424327.104-38.02 SHFK-MT-104 DIVG.424327.104-38.38	3729 - 3765	MICROSOFT WIN 10 PRO Version 1909, P/N: FQC-08909-D
SHFK-MT-104 DIVG.424327.104-38.39 SHFK-MT-104 DIVG.424327.104-38.58	3794 - 3813	MICROSOFT WIN 10 PRO Version 1909, P/N: FQC-08909-D

Schneider Electric Security Notification

SHFK-MT-104 DIVG.424327.104-38.59 SHFK-MT-104 DIVG.424327.104-38.78	3815 - 3834	MICROSOFT WIN 10 PRO Version 1909, P/N: FQC-08909-D
SHFK-MT-104 DIVG.424327.104-38.79 SHFK-MT-104 DIVG.424327.104-39.13	3835 - 3867	MICROSOFT WIN 10 PRO Version 1909, P/N: FQC-08909-D
SHFK-MT-104 DIVG.424327.104-40	3814	MICROSOFT WIN 10 PRO, P/N: FQC-08909-D
SHFK-MT-104 DIVG.424327.104-45	3822	MICROSOFT WIN 10 PRO Version 1909, P/N: FQC-08909-D

Vulnerability Details

CVE ID: **CVE-2021-31166**

CVSS v3.0 Base Score 9.8 | Critical | CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

HTTP Protocol Stack Remote Code Execution Vulnerability. In most situations, an unauthenticated attacker could send a specially crafted packet to a targeted server utilizing the HTTP Protocol Stack (http.sys) to process packets.

Remediation

The Microsoft Windows® operating system updates address the vulnerabilities for all the affected products listed in this notification are available for download here:

- CVE-2021-31166: https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-31166

A reboot will be needed after the updates are applied.

Customers should use appropriate patching methodologies when applying these patches to their systems. We strongly recommend the use of back-ups and evaluating the impact of these patches in a Test and Development environment or on an offline infrastructure. Contact Schneider Electric's Customer Care Center if you need assistance removing a patch.

If customers choose not to apply the remediation provided above, they should follow the recommendations listed in the General Security Recommendations section below to reduce the risk of exploit.

General Security Recommendations

We strongly recommend the following industry cybersecurity best practices.

- Locate control and safety system networks and remote devices behind firewalls and isolate them from the business network.
- Install physical controls so no unauthorized personnel can access your industrial control and safety systems, components, peripheral equipment, and networks.
- Place all controllers in locked cabinets and never leave them in the "Program" mode.

- Never connect programming software to any network other than the network for the devices that it is intended for.
- Scan all methods of mobile data exchange with the isolated network such as CDs, USB drives, etc. before use in the terminals or any node connected to these networks.
- Never allow mobile devices that have connected to any other network besides the intended network to connect to the safety or control networks without proper sanitation.
- Minimize network exposure for all control system devices and systems and ensure that they are not accessible from the Internet.
- When remote access is required, use secure methods, such as Virtual Private Networks (VPNs). Recognize that VPNs may have vulnerabilities and should be updated to the most current version available. Also, understand that VPNs are only as secure as the connected devices.

For more information refer to the Schneider Electric Recommended Cybersecurity Best Practices document.

For More Information

This document provides an overview of the identified vulnerability or vulnerabilities and actions required to mitigate. For more details and assistance on how to protect your installation, contact your local Schneider Electric representative or Schneider Electric Industrial Cybersecurity Services: https://www.se.com/ww/en/work/solutions/cybersecurity/. These organizations will be fully aware of this situation and can support you through the process.

For further information related to cybersecurity in Schneider Electric's products, visit the company's cybersecurity support portal page:
https://www.se.com/ww/en/work/support/cybersecurity/overview.jsp

Schneider Electric Security Notification

About Schneider Electric

At Schneider, we believe **access to energy and digital** is a basic human right. We empower all to **do more with less**, ensuring **Life Is On** everywhere, for everyone, at every moment.

We provide **energy and automation digital** solutions for **efficiency and sustainability.** We combine world-leading energy technologies, real-time automation, software and services into integrated solutions for Homes, Buildings, Data Centers, Infrastructure and Industries.

We are committed to unleash the infinite possibilities of an **open, global, innovative community** that is passionate with our **Meaningful Purpose, Inclusive and Empowered** values.

www.se.com

Revision Control

Version 1.0 *10 August 2021*	Original Release

Product Security Office

Digitally signed by Product Security Office
Date: 2021.08.07 21:22:36 -04'00'