

Schneider Electric Security Notification

Harmony HMI and Pro-face HMI products

10 December 2024

Overview

Schneider Electric is aware of a vulnerability in its Harmony HMIST6, HMISTM6, HMIG3U, HMIG3X, HMISTO7 products used with EcoStruxure™ Operator Terminal Expert Software and PFXST6000, PFXSTM6000, PFXSP5000, PFXGP4100 products used with Pro-face BLUE Software.

[Harmony HMI Panels](#) and [Pro-face HMI Panels](#) are the main visible automation component that manage all vital machine features, including visualization, control, supervision, diagnostics, monitoring, and data logging.

Failure to apply the mitigations provided below may risk various attack scenarios due to Third-Party Component obsolescence, which could result in complete loss of control, Integrity and Confidentiality of the device and operational failure.

Affected Products and Versions

Product	Version
Harmony (Formerly Magelis) HMIST6, HMISTM6, HMIG3U, HMIG3X, HMISTO7 series with EcoStruxure™ Operator Terminal Expert runtime	All versions
PFXST6000, PFXSTM6000, PFXSP5000, PFXGP4100 series with Pro-face BLUE runtime	All versions

Vulnerability Details

CVE ID: CVE-2024-11999

CVSS v3.1 Base Score 8.8 | High | CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

CVSS v4.0 Base Score 8.7 | High | CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N

CWE-1104: Use of Unmaintained Third-Party Components vulnerability exists that could cause complete control of the device when an authenticated user installs malicious code into HMI product.

The severity of vulnerabilities was calculated using the CVSS Base metrics for 4.0 ([CVSS v4.0](#)). CVSS v3.1 will be still evaluated until the adoption of CVSS v4.0 by the industry. The severity was calculated without incorporating the Temporal and Environmental metrics. Schneider Electric recommends that customers score the CVSS Environmental metrics, which are specific to end-user organizations, and consider factors such as the presence of mitigations in that environment. Environmental metrics may refine the relative severity posed by the vulnerabilities described in this document within a customer's environment.

Schneider Electric Security Notification

Mitigations

Affected Product & Version	Mitigations
<p>Harmony (Formerly Magelis) HMIST6, HMISTM6, HMIG3U, HMIG3X, HMISTO7 series with EcoStruxure™ Operator Terminal Expert runtime</p> <p>PFXST6000, PFXSTM6000, PFXSP5000, PFXGP4100 series with Pro-face BLUE runtime</p> <p><i>All versions</i></p>	<p>Customers should immediately apply the following mitigations to reduce the risk of exploit:</p> <ul style="list-style-type: none">• Use HMI only in a protected environment to minimize network exposure and ensure that they are not accessible from public internet or untrusted networks.• Setup network segmentation and implement a firewall to block all unauthorized access.• Restrict usage of unverifiable portable media• Restricting the application access to limit the transfer of Firmware to HMI• Scanning of software/files for rootkits before usage and verifying the digital signature.• When exchanging files over the network, use secure communication protocols. <p>To ensure you are informed of all updates, including details on affected products and remediation plans, subscribe to Schneider Electric's security notification service here: https://www.se.com/en/work/support/cybersecurity/security-notifications.jsp</p>

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 intended for that device.
- 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.

Schneider Electric Security Notification

- 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>

LEGAL DISCLAIMER

THIS NOTIFICATION DOCUMENT, THE INFORMATION CONTAINED HEREIN, AND ANY MATERIALS LINKED FROM IT (COLLECTIVELY, THIS "NOTIFICATION") ARE INTENDED TO HELP PROVIDE AN OVERVIEW OF THE IDENTIFIED SITUATION AND SUGGESTED MITIGATION ACTIONS, REMEDIATION, FIX, AND/OR GENERAL SECURITY RECOMMENDATIONS AND IS PROVIDED ON AN "AS-IS" BASIS WITHOUT WARRANTY OR GUARANTEE OF ANY KIND. SCHNEIDER ELECTRIC DISCLAIMS ALL WARRANTIES RELATING TO THIS NOTIFICATION, EITHER EXPRESS OR IMPLIED, INCLUDING WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. SCHNEIDER ELECTRIC MAKES NO WARRANTY THAT THE NOTIFICATION WILL RESOLVE THE IDENTIFIED SITUATION. IN NO EVENT SHALL SCHNEIDER ELECTRIC BE LIABLE FOR ANY DAMAGES OR LOSSES WHATSOEVER IN CONNECTION WITH THIS NOTIFICATION, INCLUDING DIRECT, INDIRECT, INCIDENTAL, CONSEQUENTIAL, LOSS OF BUSINESS PROFITS OR SPECIAL DAMAGES, EVEN IF SCHNEIDER ELECTRIC HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. YOUR USE OF THIS NOTIFICATION IS AT YOUR OWN RISK, AND YOU ARE SOLELY LIABLE FOR ANY DAMAGES TO YOUR SYSTEMS OR ASSETS OR OTHER LOSSES THAT MAY RESULT FROM YOUR USE OF THIS NOTIFICATION. SCHNEIDER ELECTRIC RESERVES THE RIGHT TO UPDATE OR CHANGE THIS NOTIFICATION AT ANY TIME AND IN ITS SOLE DISCRETION.

About Schneider Electric

Schneider's purpose is to empower all to make the most of our energy and resources, bridging progress and sustainability for all. We call this Life Is On.

Our mission is to be your digital partner for Sustainability and Efficiency.

We drive digital transformation by integrating world-leading process and energy technologies, end-point to cloud connecting products, controls, software and services, across the entire lifecycle, enabling integrated company management, for homes, buildings, data centers, infrastructure and industries.

We are the most local of global companies. We are advocates of open standards and partnership ecosystems that are passionate about our shared Meaningful Purpose, Inclusive and Empowered values.

www.se.com

Schneider Electric Security Notification

Revision Control:

Version 1.0.0 <i>10 December 2024</i>	Original Release
-------------------------------------------------	------------------