REVISION: 1
PUBLICATION DATE: 2022-09-06
DOC. IDENTIFIER: 8DBD000106
PUBLISHER: HITACHI ENERGY PSIRT
DOCUMENT STATUS: FINAL

HITACHI
Inspire the Next

CYBERSECURITY ADVISORY

Multiple Vulnerabilities in Hitachi Energy's MicroSCADA Pro/X SYS600 Products

CVE-2022-1778
CVE-2022-2277
CVE-2022-29922
CVE-2022-29490
CVE-2022-29492

Notice

The information in this document is subject to change without notice and should not be construed as a commitment by Hitachi Energy. Hitachi Energy provides no warranty, express or implied, including warranties of merchantability and fitness for a particular purpose, for the information contained in this document, and assumes no responsibility for any errors that may appear in this document. In no event shall Hitachi Energy or any of its suppliers be liable for direct, indirect, special, incidental or consequential damages of any nature or kind arising from the use of this document, or from the use of any hardware or software described in this document, even if Hitachi Energy or its suppliers have been advised of the possibility of such damages. This document and parts hereof must not be reproduced or copied without written permission from Hitachi Energy and the contents hereof must not be imparted to a third party nor used for any unauthorized purpose. All rights to registrations and trademarks reside with their respective owners.

© Copyright 2022 Hitachi Energy. All rights reserved.

Hitachi Energy

Summary

Hitachi Energy is aware of internal reports of multiple vulnerabilities in the MicroSCADA Pro/X SYS600 versions as described in the Recommended Immediate Actions Section below. An update is available that resolves the reported vulnerabilities.

An attacker who successfully exploited the vulnerabilities, depends on the vulnerabilities, could cause SYS600 fail to start, unauthorized actor to run scripts, and may cause a denial-of-service.

Vulnerability ID, Severity and Details

The vulnerability's severity assessment is performed by using the FIRST Common Vulnerability Scoring System (CVSS) v3.1. The CVSS Environmental Score, which can affect the final vulnerability severity score, is not provided in this advisory as it reflects the potential impact of the vulnerability in the customer organizations' computing environment. Customers are recommended to analyze the impact of the vulnerability in their environment and calculate the CVSS Environmental Score.

Vulnerability ID	Detail Description
CVE-2022-1778 CVSS v3.1 Base Score: 7.5 High CVSS v3.1 Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/ Link to NVD: click here CWE-20: Improper Input Validation	A vulnerability exists during the start of SYS600, where an input validation flaw causes a buffer-overflow while reading a specific configuration file. Subsequently SYS600 will fail to start. The configuration file can only be accessed by an administrator access.
CVE-2022-2277 CVSS v3.1 Base Score: 7.5 High CVSS v3.1 Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/ Link to NVD: click here CWE-20: Improper Input Validation	A vulnerability exists in the ICCP stack due to validation flaw in the process that establishes the ICCP communication. The validation flaw will cause a denial-of-service when ICCP of SYS600 is request to forward any data item updates with timestamps too distant in the future to any remote ICCP system. By default, ICCP is not configured and not enabled.
CVE-2022-29490 CVSS v3.1 Base Score: 8.5 High CVSS v3.1 Vector: AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/ Link to NVD: click here	A vulnerability exists in the Workplace X WebUI in which an authenticated user is able to execute any MicroSCADA internal scripts irrespective of the authenticated user's role.
CVE-2022-29492 CVSS v3.1 Base Score: 5.3 Medium CVSS v3.1 Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L/ Link to NVD: click here	A vulnerability exists in the handling of a malformed IEC 104 TCP packet. Upon receiving a malformed IEC 104 TCP packet, the malformed packet is dropped, however the TCP connection is left open. This may cause a denial-of-service if the affected connection is left open.
CVE-2022-29922 CVSS v3.1 Base Score: 7.5 High CVSS v3.1 Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/ Link to NVD: click here	A vulnerability exists in the handling of a specially crafted IEC 61850 packet with a valid data item but with incorrect data type in the IEC 61850 OPC Server. The vulnerability may cause a denial-of-service on the IEC 61850 OPC Server part of the SYS600 product.

© Copyright 2022 Hitachi Energy. All rights reserved.

Recommended Immediate Actions

The Table below shows the affected version and the recommended immediate actions.

Vulnerabilities	Affected Version	Recommended Actions
CVE-2022-1778	SYS600 10.0 - 10.3.1	Remediated in SYS600 10.4 Update to at least SYS600 version 10.4. Or apply general mitigation factors
CVE-2022-2277	SYS600 10.2.0 – 10.3.1	Remediated in SYS600 10.4 Update to at least SYS600 version 10.4. Or apply general mitigation factors Do not enable ICCP if it is not used
CVE-2022-29490	SYS600 10.0 - 10.3.1	Remediated in SYS600 10.4 Update to at least SYS600 version 10.4. Or apply general mitigation factors
CVE-2022-29492 CVE-2022-29922	SYS600 10.3.1 and earlier SYS600 9.4 FP2 Hotfix 4 and any earlier versions	Remediated in SYS600 10.4 For SYS600 9.x upgrade to at least SYS600 version 10.4. For SYS600 10.x update to at least SYS600 version 10.4. Or apply general mitigation factors

Hitachi Energy recommends that customers apply the update at the earliest convenience.

General Mitigation Factors/Workarounds

Recommended security practices and firewall configurations can help protect a process control network from attacks that originate from outside the network. Such practices include that process control systems are physically protected from direct access by unauthorized personnel, have no direct connections to the Internet, and are separated from other networks by means of a firewall system that has a minimal number of ports exposed, and others that have to be evaluated case by case. Process control systems should not be used for Internet surfing, instant messaging, or receiving e-mails. Portable computers and removable storage media should be carefully scanned for viruses before they are connected to a control system. Proper password policies and processes should be followed.

We recommend following the cybersecurity deployment guideline as follows:

1MRK511518 MicroSCADA X Cyber Security Deployment Guideline

Frequently Asked Questions

What is SYS600?

SYS600 is a SCADA product, which is used for monitoring and controlling power systems.

What might an attacker use the vulnerability to do?

An attacker who successfully exploited the CVE-2022-1778 could cause a failure in starting SYS600. When CVE-2022-29490 vulnerability is exploited, an attacker could run an administrator level script that could provide the attacker access to information and to cause a disruption in SYS600 operation. For the CVE-2022-2277,

© Copyright 2022 Hitachi Energy. All rights reserved.

CVE-2022-29492 and CVE-2022-29922, upon successful exploitation, an attacker could cause a denial-of-service on the respective function in SYS600.

How could an attacker exploit the vulnerability?

To exploit CVE-2022-1778, an attacker needs to have a local access to the SYS600 and an administrator account is required.

For CVE-2022-2277, if ICCP is configured and enabled in SYS600, an attacker needs to send data item updates with timestamps too distant in the future to a SYS600 server which is configured to forward the data via ICCP to other ICCP clients.

For CVE-2022-29490, an attacker needs to first authenticate to the system. After successful login attacker can exploit affected components by sending specially crafted messages.

CVE-2022-29492 and CVE-2022-29922, can be exploited without authentication by sending malicious packets over the network towards the affected SYS600 instance.

Recommended practices help mitigate such attacks, see section Mitigating Factors above.

Could the vulnerability be exploited remotely?

For CVE-2022-1778, an attacker needs to gain an access to the server where SYS600 is installed.

For CVE-2022-29490, an attacker is required to access the web interface and to have a valid user account to exploit it. This vulnerability is not bound to a network stack.

For the CVE-2022-2277, CVE-2022-29492 and CVE-2022-29922, these vulnerabilities are bound to a network stack. This means, exploitation would require that the attacker has access to the system network, by connecting to the network either directly or through a wrongly configured or penetrated firewall, or that he installs malicious software on a system node or otherwise infects the network with malicious software. Recommended practices include that process control systems are physically protected, have no direct connections to the Internet, and are separated from other networks by means of a firewall system that has a minimal number of ports exposed.

When this security advisory was issued, had this vulnerability been publicly disclosed ow could an attacker exploit the vulnerability?

No Hitachi Energy received information about this vulnerability internally.

When this security advisory was issued, had Hitachi Energy received any report that this vulnerability was being exploited?

No Hitachi Energy had not received any information indicating that these vulnerabilities had been exploited when this security advisory was originally issued.

Support

This advisory will be updated as new relevant information becomes available. Please subscribe to Hitachi Energy's Cybersecurity Alerts & Notifications to get notified:

https://www.hitachienergy.com/offering/solutions/cybersecurity/alerts-and-notifications/subscribe

For additional information and support please contact your product provider or Hitachi Energy service organization. For contact information, see https://www.hitachienergy.com/contact-us/ for Hitachi Energy contact-centers.

© Copyright 2022 Hitachi Energy. All rights reserved.

Publisher

Hitachi Energy PSIRT – cybersecurity@hitachienergy.com

Revision

Date of the Revision	Revision	Description
2022-09-06	1	Initial public release.

DocuSigned by:

© Copyright 2022 Hitachi Energy. All rights reserved.