TLP: CLEAR
REVISION: 1
PUBLICATION DATE: 2022-11-15
DOC. IDENTIFIER: 8DBD000123
PUBLISHER: HITACHI ENERGY PSIRT
DOCUMENT STATUS: FINAL

HITACHI
Inspire the Next

CYBERSECURITY ADVISORY

Input Validation Vulnerability in Hitachi Energy's MicroSCADA Pro/X SYS600 Products

CVE-2022-3388

Notice

Hitachi Energy

Summary

Hitachi Energy is aware of internal reports of an input validation vulnerability that exists in the Monitor Pro interface of MicroSCADA Pro and MicroSCADA X SYS600. An update is available that resolves the reported vulnerabilities.

An authenticated user who successfully exploits the vulnerability, could execute administrator level scripts on SYS600. Note that exploitation is only possible if the attacker manages to login to the SYS600.

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-2022-3388 CVSS v3.1 Base Score: 8.8 High CVSS v3.1 Vector: AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H Link to NVD: click here CWE-20: Improper Input Validation	An input validation vulnerability exists in the Monitor Pro interface of MicroSCADA Pro and MicroSCADA X SYS600. An authenticated user can launch an administrator level remote code execution irrespective of the authenticated user's role.

Recommended Immediate Actions

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

Vulnerabilities	Affected Version	Recommended Actions
CVE-2022-3388	SYS600 10.4 and earlier SYS600 9.4 FP2 Hotfix 4 and any earlier versions	• For SYS600 9.x: update to at SYS600 version SYS600 9.4 FP2 Hotfix 5 when it is released or upgrade to at least SYS600 version 10.4.1. A requirement to install SYS600 9.4 FP2 Hotfix 5 is to have at least the SYS600 9.4 FP2 Hotfix 4 installed. • For SYS600 10.x update to at least SYS600 version 10.4.1 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, after successfully being authenticated on SYS600, could launch an administrator level remote code execution on SYS600.

How could an attacker exploit the vulnerability?

An attacker needs to first authenticate to the system. Recommended practices help mitigate such attacks, see section Mitigating Factors above.

Could the vulnerability be exploited remotely?

For CVE-2022-3388, an attacker is required to access to the SYS600 and a valid user account to exploit it. This vulnerability is not bound to a network stack.

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

No Hitachi Energy received information about this vulnerability privately.

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.

Publisher

Hitachi Energy PSIRT – cybersecurity@hitachienergy.com

Revision

Date of the Revision	Revision	Description
2022-11-15	1	Initial public release.

DocuSigned by: