REVISION: A
PUBLICATION DATE: 2022-01-20
DOC. IDENTIFIER: 8DBD000075
PUBLISHER: HITACHI ENERGY PSIRT
DOCUMENT STATUS: FINAL

HITACHI
Inspire the Next

CYBERSECURITY ADVISORY

# Multiple Open-Source Software Related Vulnerabilities in Hitachi Energy MicroSCADA Pro/X SYS600 Products

CVE-2020-1968
CVE-2020-8265
CVE-2020-8201
CVE-2020-8252
CVE-2020-8287
CVE-2020-8172
CVE-2020-8174
CVE-2021-32027
CVE-2021-32028

## Notice





Hitachi Energy

# Summary

Hitachi Energy is aware of internal reports of multiple open-source software related vulnerabilities in the SYS600 product versions listed in this document. Remediated versions are available that remediate the identified vulnerabilities.

An attacker who successfully exploited this vulnerability could eavesdrop on the traffic between network source and destination, gain unauthorized access to information or 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.

## OpenSSL

| CVE-ID | Severity, Vector and Link to NVD |
|---|---|
| **CVE-2020-1968** | CVSS v3.1 Base Score: 3.7 Low<br>CVSS v3.1 Vector: /AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N<br>Link to NVD: click here |

## Node.JS

| CVE-ID | Severity, Vector and Link to NVD |
|---|---|
| **CVE-2020-8265** | CVSS v3.1 Base Score: 8.1 High<br>CVSS v3.1 Vector: /AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H<br>Link to NVD: click here |
| **CVE-2020-8287** | CVSS v3.1 Base Score: 6.5 Medium<br>CVSS v3.1 Vector: /AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N<br>Link to NVD: click here |
| **CVE-2020-8201** | CVSS v3.1 Base Score: 7.4 High<br>CVSS v3.1 Vector: /AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N<br>Link to NVD: click here |
| **CVE-2020-8252** | CVSS v3.1 Base Score: 7.8 High<br>CVSS v3.1 Vector: AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H<br>Link to NVD: click here |
| **CVE-2020-8172** | CVSS v3.1 Base Score: 7.4 High<br>CVSS v3.1 Vector: /AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N<br>Link to NVD: click here |
| **CVE-2020-8174** | CVSS v3.1 Base Score: 8.1 High<br>CVSS v3.1 Vector: /AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H<br>Link to NVD: click here |

### PostgreSQL

| CVE-ID | Severity, Vector and Link to NVD |
|---|---|
| **CVE-2021-32027** | CVSS v3.1 Base Score: 8.8 High<br>CVSS v3.1 Vector: /AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H<br>Link to NVD: click here |
| **CVE-2021-32028** | CVSS v3.1 Base Score: 6.5 Medium<br>CVSS v3.1 Vector: /AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N<br>Link to NVD: click here |

Below follows a summary regarding the possible impact of the identified vulnerabilities:

- **OpenSSL vulnerability**: Exploitation of the OpenSSL Raccoon attack may allow an attacker to compute the pre-master secret between the client and server in connections which have used a Diffie-Hellman (DH) based cipher suite and thus able to eavesdrop on all encrypted communications sent over that TLS connection.
- **Node.js vulnerabilities:** Exploitation may cause a denial-of-service to the system, data extraction by various methods, bypass the hostname checks in TLS connections or memory corruption.
- **PostgreSQL vulnerabilities:** Authenticated users can read/write arbitrary bytes from/to a wide area of the server memory.

## Affected Product Versions & Recommended Immediate Actions

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

| Vulnerabilities | Affected Version | Recommended Actions |
|---|---|---|
| ***OpenSSL Vulnerability*** | SYS600 10.1.1 and earlier | Remediated in SYS600 10.2.<br>For SYS600 9.x upgrade to at least SYS600 version 10.2.<br>For SYS600 10.x update to at least SYS600 version 10.2.<br>Or apply general mitigation factors. |
| ***Node.js vulnerabilities*** | SYS600 9.4 FP1 – 10.2.1 | Remediated in SYS600 10.3.<br>For SYS600 9.x upgrade to at least SYS600 version 10.3.<br>For SYS600 10.x update to at least SYS600 version 10.3.<br>Or apply general mitigation factors. |
| ***PostgreSQL vulnerabilities*** | SYS600 10.0.0 – 10.2.1 | Remediated in SYS600 10.3.<br>For SYS600 9.x upgrade to at least SYS600 version 10.3.<br>For SYS600 10.x update to at least SYS600 version 10.3.<br>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.

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 this vulnerability could eavesdrops on the traffic, cause the affected system node to stop or become inaccessible / allow the attacker to access to information without proper access rights.

## How could an attacker exploit the vulnerability?

An attacker could exploit the vulnerability by creating a specially crafted message and sending the message to an affected system node. Some vulnerabilities described above also require authentication to the system before they can be exploited.

Exploitation would require the attacker to have access to the system network, by connecting to the network either directly or through a wrongly configured or penetrated firewall, or through an installed malicious software on a system node. Recommended practices help to mitigate such attacks, see section Mitigating Factors above.

## Could the vulnerability be exploited remotely?

Yes, an attacker who has a network access to an affected system node could exploit this vulnerability. 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?

Yes, these vulnerabilities have been publicly disclosed by the respective Open-Source Software teams.

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

No, at the date of this advisory publication Hitachi Energy had not received any information indicating that this vulnerability had been exploited.

# Support

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 |
|---|---|---|
| 2022-01-20 | A | Initial public release. |