REVISION: A
PUBLICATION DATE: 2021-12-21
DOC. IDENTIFIER: 8DBD000074
PUBLISHER: HITACHI ENERGY PSIRT
DOCUMENT STATUS: FINAL

HITACHI
Inspire the Next

CYBERSECURITY ADVISORY

Multiple Open-Source Software Related Vulnerabilities in Hitachi Energy System Data Manager (SDM600) Product

CVE-2020-1968
CVE-2020-12243
CVE-2020-25709
CVE-2020-25710
CVE-2020-36229
CVE-2020-36230
CVE-2021-23840

Notice

Hitachi Energy

Summary

Hitachi Energy is aware of vulnerability reports on multiple open-source software that is used in the System Data Manager (SDM600) product versions listed below. An update that remediates the vulnerabilities is available.

An attacker who successfully exploited this vulnerability could eavesdrops on the traffic or to cause a denial-of-service.

Affected Products and Versions

All System Data Manager – SDM600 versions prior to version 1.2 FP2 HF10 (Build Nr. 1.2.14002.506)

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-2020-1968 CVSS v3.1 Base Score: 3.7 Low CVSS v3.1 Vector: /AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N Link to NVD: click here	**OpenSSL:** In the affected OpenSSL versions, the Raccoon attack exploits a flaw in the TLS specification which can lead to an attacker being able to compute the pre-master secret in connections which have used a Diffie-Hellman (DH) based ciphersuite and then eavesdrop on all encrypted communications sent over that TLS connection.
CVE-2020-12243 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	**OpenLDAP:** In the affected versions of OpenLDAP, LDAP search filters with nested boolean expressions can result in denial-of-service.
CVE-2020-25709 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	**OpenLDAP:** A flaw in the affected versions of OpenLDAP versions' slapd server may cause an assertion failure when processing a malicious packet. This may lead to a denial-of-service.
CVE-2020-25710 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	**OpenLDAP:** A flaw in the affected versions of OpenLDAP allows an attacker who sends a malicious packet processed by OpenLDAP to force a failed assertion in csnNormalize23() function. This may lead to a denial-of-service.
CVE-2020-36229 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	**OpenLDAP:** A flaw was discovered in ldap_X509dn2bv in the affected OpenLDAP versions leading to a slapd crash in the X.509 DN parsing in ad_keystring, resulting in denial-of-service.

CVE-2020-36230 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	**OpenLDAP:** A flaw was discovered in the affected OpenLDAP versions leading in an assertion failure in slapd in the X.509 DN parsing in decode.c ber_next_element, resulting in denial-of-service.
CVE-2021-23840 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	**OpenSSL:** A flaw in the affected versions of OpenSSL may cause calls to EVP_CipherUpdate, EVP_EncryptUpdate and EVP_DecryptUpdate to overflow the output length argument in some cases where the input length is close to the maximum permissable length for an integer on the platform. This could lead to applications behaving incorrectly.

The impact of the documented vulnerabilities are as follows:

– **Decryption of TLS traffic:** 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 ciphersuite.

– **Denial-of-service:** An attacker with access to the network can exploit the vulnerabilities related to OpenLDAP component resulting in a possibility of denial-of-service.

Recommended Immediate Actions

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

Affected Version	Recommended Actions
All SDM600 versions prior to version 1.2 FP2 HF10 (Build Nr. 1.2.14002.506)	The problem is remediated as of the following product version SDM600 version 1.2 FP2 HF10 (Build Nr. 1.2.14002.506). Hitachi Energy recommends that customers apply the update at the earliest convenience. The download can be obtained from the SDM600 product website.

General Mitigation Factors/Workarounds

It is recommended to implement and continuously revise least privileges principles to minimize permissions and accesses to SDM600 related resources. Furthermore, recommended security practices as defined in SDM600 security deployment guideline and firewall configurations can help to 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.

Additional recommendation is to follow the hardening guidelines published by “The Center for Internet Security (CIS)” https://www.cisecurity.org/about-us/ to protect the host Operating System

Frequently Asked Questions

What is System Data Manager (SDM600)?

SDM600 (System Data Manager) is a comprehensive software solution for automatic management of service and cyber security relevant data across your substations. SDM600 is based on flexible and remotely accessible system architecture. It provides you with efficient data and user management of all stations from one central point.

What might an attacker use the vulnerability to do?

The vulnerabilities as described in this advisory may cause:

- Decryption of TLS traffic which results in traffic eavesdropping
- A denial-of-service on SDM600.

Could the vulnerability be exploited remotely?

Yes, an attacker who has 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, the vulnerabilities of the open-source software 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, Hitachi Energy had not received any information indicating that this vulnerability had been exploited when this security advisory was originally issued.

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[1] – cybersecurity@hitachienergy.com

[1] Signature file of this PDF is available at https://www.hitachienergy.com/cybersecurity/alerts-and-notifications

Revision

Date of the Revision	Revision	Description
2021-12-21	A	Initial public release.