REVISION: A
PUBLICATION DATE: 2022-01-13
DOC. IDENTIFIER: 8DBD000077
PUBLISHER: HITACHI ENERGY PSIRT
DOCUMENT STATUS: FINAL

HITACHI
Inspire the Next

CYBERSECURITY ADVISORY

Multiple Vulnerabilities Related to Open-Source Software in Hitachi Energy e-mesh™ Energy Management System (EMS) Product

CVE-2020-8174 CVE-2020-11080
CVE-2020-8265 CVE-2021-22883

Notice

Hitachi Energy

Summary

Hitachi Energy is aware of internal report of Open-Source Software Node.js related vulnerabilities in the e-mesh Energy Management System (EMS) product version listed below. An update is available that resolves the vulnerabilities in the product versions listed above.

An attacker who successfully exploited this vulnerability could cause a denial-of-service on the product.

Affected Products and Versions

List of affected products and product versions:

– e-mesh EMS 1.0

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-2020-8174; CVSS v3.1 Base Score: 8.1 High CVSS v3.1 Vector: /AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H Link to NVD: click here	**Node.js vulnerability** – Function napi_get_value_string_*() in the affected versions of Node.js allows various kinds of memory corruption.
CVE-2020-8265; CVSS v3.1 Base Score: 8.1 High CVSS v3.1 Vector: /AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H Link to NVD: click here	**Node.js vulnerability** – The affected versions of Node.js are vulnerable to a use-after-free bug in its TLS implementation. Exploitation of this vulnerability may corrupt memory leading to a denial-of-service.
CVE-2020-11080; 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	**Node.js vulnerability** – The affected versions of Node.js are vulnerable to a denial-of-service, due to an error in the HTTP/2 session frame which is limited to 32 settings by default. By sending overly large HTTP/2 SETTINGS frames, an attacker could exploit this vulnerability to consume all available CPU resources.
CVE-2021-22883; 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	**Node.js vulnerability** – The affected versions of Node.js is vulnerable to a denial-of-service attack when too many connection attempts with an 'unknownProtocol' are established.

The following lists the following possible impact of those vulnerabilities:

– **Denial-of-service:** Exploitation of the vulnerabilities may cause a denial-of-service on the e-mesh EMS product.

Recommended Immediate Actions

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

Affected Version	Recommended Actions
e-mesh EMS 1.0	e-mesh EMS 1.0.1

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.

Frequently Asked Questions

What is e-mesh Energy Management System (EMS)?

Hitachi Energy e-mesh EMS is an optimizer software focused on optimally dispatching a set of distributed energy resources at the lowest operational costs in any multi variable governed environment leveraging on intra-day and day ahead optimizations. additional features for the energy management of distributed energy resources. E-mesh EMS application integrates renewables, conventional power generation sources, and loads like electrical vehicle (EV) chargers.

What might an attacker use the vulnerability to do?

An attacker who successfully exploited this vulnerability could cause a denial-of-service on the product.

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 on 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

Revision

Date of the Revision	Revision	Description
2022-01-13	A	Initial public release.

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