

CYBERSECURITY ADVISORY

OpenLDAP Related Vulnerabilities in Hitachi Energy RTU500 series

CVE-2020-36229
CVE-2020-36230

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.

Summary

Hitachi Energy is aware of internal reports of OpenLDAP related vulnerabilities in the RTU500 series versions listed below. Recommended action for each affected version is listed in the Recommended Immediate Actions Section.

An attacker could exploit this vulnerability only on RTU500 series in which Central Account Management (CAM) function is configured and enabled by project configuration. Note that CAM function is disabled (not configured) by default. An attacker who successfully exploited this vulnerability could cause a denial-of-service to the affected versions of the RTU500 series product.

Affected Products and Versions

List of affected products and product versions (* indicates all versions – See Recommended Immediate Actions for details):

- RTU500 series CMU Firmware version 12.4.*
- RTU500 series CMU Firmware version 12.6.*
- RTU500 series CMU Firmware version 12.7.*
- RTU500 series CMU Firmware version 13.0.*
- RTU500 series CMU Firmware version 13.1.*
- RTU500 series CMU Firmware version 13.2.1

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-2020-36229 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.

The following lists the following possible impact of those vulnerabilities:

- **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
RTU500 series CMU Firmware version 12.4.1 – 12.4.10	Please refer to the Mitigation Factors/Workaround Section for the current mitigation strategy or Update to RTU500 series CMU firmware as of version 12.4.11 (to be released by end-of-January 2022).
RTU500 series CMU Firmware version 12.6.1 – 12.6.6	Update to RTU500 series CMU firmware as of version 12.6.7.
RTU500 series CMU Firmware version 12.7.1	Update to RTU500 series CMU firmware as of version 12.7.2
RTU500 series CMU Firmware version 13.0.1 – 13.0.2	Please refer to the Mitigation Factors/Workaround Section for the current mitigation strategy or upgrade to the latest RTU500 series CMU firmware as of version 13.2.3.
RTU500 series CMU Firmware version 13.1.1 – 13.1.2	Please refer to the Mitigation Factors/Workaround Section for the current mitigation strategy or upgrade to the latest RTU500 series CMU firmware as of version 13.2.3.
RTU500 series CMU Firmware version 13.2.1	Please refer to the Mitigation Factors/Workaround Section for the current mitigation strategy or upgrade to the latest RTU500 series CMU firmware as of version 13.2.3.

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

Mitigation Factors/Workarounds

As the vulnerability affects only the RTU500 series in which CAM function is configured and enabled, a possible mitigation is to disable the CAM function if it is not used.

By default, the CAM function is disabled.

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 RTU500 series?

RTU500 series is a remote terminal unit product configurable to nearly all demands made on remote stations in networks for electrical substations, gas, oil water and district heating.

The RTU500 series therefore provides a flexible and modular design with many integrated functionalities covering a wide range of individual solutions suitable for transmission, distribution substations, smart grids or feeder automation applications.

What is the scope of the vulnerability?

The vulnerability affects only RTU500 series in which CAM function is configured and enabled by project configuration.

What might an attacker use the vulnerability to do?

The vulnerabilities as described in this advisory may cause a denial-of-service to the affected RTU500 series.

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, 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, 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 PSIRT¹ – 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
2021-11-17	A	Initial public release.
2021-12-02	B	Section Recommended Immediate Actions: <ul style="list-style-type: none">RTU500 series CMU Firmware version 12.6.7 is available.