REVISION: A
PUBLICATION DATE: 2022-03-08
DOC. IDENTIFIER: 8DBD000078
PUBLISHER: HITACHI ENERGY PSIRT
DOCUMENT STATUS: FINAL

HITACHI
Inspire the Next

CYBERSECURITY ADVISORY

Multiple Vulnerabilities Related to Open-Source Software in Hitachi Energy RelCare Product

CVE-2020-1967
CVE-2021-3156
CVE-2021-3449
CVE-2021-3450
CVE-2021-27432
CVE-2021-27434
CVE-2021-28041

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.

© Copyright 2022 Hitachi Energy. All rights reserved.

Hitachi Energy

Summary

Hitachi Energy is aware of aware of multiple vulnerabilities in Open-Source Software components that are used in the RelCare Cloud and OnPrem versions listed below. An update is available that remediated the vulnerabilities. No user action is required as the update has been deployed to both RelCare Cloud and OnPrem solutions.

An attacker who successfully exploited these vulnerabilities could cause a denial-of-service and allow unauthorized privilege escalation to root account.

Affected Products and Versions

List of affected products and product versions:

– RelCare v1.0.0

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.

CVE-ID	Severity, Vector and Link to NVD
CVE-2020-1967 **OpenSSL Vulnerability**	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
CVE-2021-3156 **Heap-Based Buffer Overflow in Sudo (Baron Samedit)**	CVSS v3.1 Base Score: 7.8 High CVSS v3.1 Vector: /AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H Link to NVD: click here
CVE-2021-3449 **OpenSSL Vulnerability**	CVSS v3.1 Base Score: 5.9 Medium CVSS v3.1 Vector: /AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H Link to NVD: click here
CVE-2021-3450 **OpenSSL Vulnerability**	CVSS v3.1 Base Score: 7.4 High CVSS v3.1 Vector: /AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N Link to NVD: click here
CVE-2021-27432 **OPC UA .NET Vulnerability**	CVSS v3.0 Base Score: 7.5 High CVSS v3.0 Vector: /AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H Link to NVD: click here
CVE-2021-27434 **OPC UA .NET Vulnerability**	CVSS v3.0 Base Score: 7.5 High CVSS v3.0 Vector: /AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N Link to NVD: click here
CVE-2021-28041 **OpenSSH Vulnerability**	CVSS v3.1 Base Score: 7.1 High CVSS v3.1 Vector: /AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H Link to NVD: click here

© Copyright 2021 Hitachi Energy. All rights reserved.

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

- **OpenSSL vulnerability**: Exploitation of the OpenSSL may cause a denial-of-service to the application.
- **Linux SUDO vulnerability**: Exploitation of this vulnerability may allow an unauthorized privilege escalation to root
- **OPC.UA .net vulnerabilities:** Exploitation may cause a denial-of-service to the system.
- **OpenSSH vulnerability:** Exploitation of this vulnerability may lead to a denial-of-service.

Recommended Immediate Actions

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

Affected Version	Recommended Actions
RelCare 1.0.0	RelCare 2.0.0 or later version remediates all the afore-mentioned vulnerabilities. No end-user action needed. Both RelCare Cloud and On-Prem version are patched to the latest version.

General Mitigation Factors/Workarounds

Recommended security practices 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 system.

Frequently Asked Questions

What is RelCare?

RelCare is a substation maintenance management system. It optimizes the substation reliability and financial key performance indicators.

What might an attacker use the vulnerability to do?

An attacker who successfully exploited these vulnerabilities could a denial-of-service and allow unauthorized escalation of privilege to root account.

How could an attacker exploit the vulnerability?

An attacker could try to exploit the vulnerabilities by creating a specially crafted message and sending the message to an affected system node. This would require that the attacker has access to the system network, by connecting to the network either directly or through a wrongly configured or penetrated firewall, or that he installs malicious software on a system node or otherwise infects the network with malicious software. Recommended practices help mitigate such attacks, see section Mitigating Factors above

© Copyright 2021 Hitachi Energy. All rights reserved.

When this security advisory was issued, had this vulnerability been publicly disclosed?

Yes, the vulnerabilities related to the Open-Source Software have been publicly disclosed by the respective Open-Source community.

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

While an exploit to the CVE-2021-3156 Linux x64 is available [1] Hitachi Energy does not have information to indicate Hitachi's Energy's products have been exploited.

References

1. https://github.com/worawit/CVE-2021-3156

Support

For additional information and support please contact your product provider or Hitachi Energy service organization. For contact information, see https://www.hitachiabb-powergrids.com/contact-us/ for Hitachi Energy contact-centers.

Publisher

Hitachi Energy PSIRT – cybersecurity@hitachienergy.com

Revision

Date of the Revision	Revision	Description
2022-03-08	A	Initial public release.

© Copyright 2021 Hitachi Energy. All rights reserved.