REVISION: A
PUBLICATION DATE: 2021-10-26
DOC. IDENTIFIER: 8DBD000056
PUBLISHER: HITACHI ENERGY PSIRT
DOCUMENT STATUS: FINAL

HITACHI
Inspire the Next

CYBERSECURITY ADVISORY

Certificate Verification Vulnerability in Update Manager of Hitachi Energy PCM600 Engineering Tool

CVE-2021-22278

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 a private report of a vulnerability in certificate's common name validation in the PCM600's Update Manager versions listed below. An update is available that remediates the reported vulnerability.

An attacker who successfully exploited this vulnerability in the PCM600's Update Manager could bypass the certificate validation and install an untrusted software package that is signed using a certificate from a trusted certificate root authority and contains the allowed patterns inside the common name.

Affected Products and Versions

Please note that Update Manager is delivered as part of PCM600 and can be updated along with PCM600 installation or separately by using Update Manager.exe. The Update Manager has its own version number.

The following Table lists the affected products and product versions.

Affected Version	Corresponding/Delivered as Part of PCM600 Version
Update Manager v2.1 Update Manager v2.1.0.4	PCM600 v2.7 and its Hotfixes
Update Manager v2.2 Update Manager v2.2.0.1 Update Manager v2.2.0.2	PCM600 v2.8 and its Hotfixes
Update Manager v2.2.0.23 Update Manager v2.3.0.60	PCM600 v2.9 and its Hotfixes
Update Manager v2.4.20041.1 Update Manager v2.4.20119.2	PCM600 v2.10 and its Hotfixes

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-2021-22278 CVSS v3.1 Base Score: 6.7 Medium CVSS v3.1 Vector: AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H Link to NVD: click here	A vulnerability exists due to logic error in the certificate validation in the Update Manager of the PCM600 version listed above. An attacker, who has an administrator rights, could exploit the vulnerabilities by creating own software packages and sign those packages with specially crafted certificates and point the PCM600 update server location to an own server location. Subsequently, due to this vulnerability, the validation flaw causes such untrusted software packages to be installed using PCM600 Update Manager.

Recommended Immediate Actions

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

Affected Version	Recommended Actions
Update Manager v2.1 Update Manager v2.1.0.4 installed with PCM600 v2.7 and its Hotfixes	Update the PCM600's Update Manager to Update Manager v2.4.21218.1. This can be done by checking directly on the Recommended Updates in the PCM600's Update Manager or by downloading it from the following link: https://www143.abb.com/SoftwareLibrary
Update Manager v2.2 Update Manager v2.2.0.1 Update Manager v2.2.0.2 installed with PCM600 v2.8 and its hotfixes	
Update Manager v2.2.0.23 Update Manager v2.3.0.60 installed with PCM600 v2.9 and its hotfixes	
Update Manager v2.4.20041.1 Update Manager v2.4.20119.2 installed with PCM600 v2.10 and its hotfixes	

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.

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 PCM600 Update Manager?

Product PCM600 is a tool that provides versatile functionalities for the entire life cycle of all Relion® protection and control IED applications, at all voltage levels. The tool helps the user to manage the Relion® protection and control equipment all the way from application and communication configuration to disturbance handling, including automatic disturbance reporting. PCM600 comes with Update Manager, and Update Manager is used for managing the current installation of PCM600 and Connectivity Packages, for notifying about available updates and for downloading/installing the updates.

What might an attacker use the vulnerability to do?

An attacker who successfully exploited this vulnerability could get untrusted/unauthorized software packages to be installed on computer where PCM600 is installed.

How could an attacker exploit the vulnerability?

An attacker, who has an administrator access to the PCM600 workstation, can sign an untrusted PCM600 package that is not officially issued by us using a certificate from a trusted root authority in which the common name matches any certain patterns allowed in the pattern validation flaw. In addition, it is required to point the PCM600 update server location to an own server. Then the signed software packages can then be installed by a user with administrator access to the PCM600 workstation.

Could the vulnerability be exploited remotely?

No, to exploit this vulnerability an attacker would need to have a physical and administrator access PCM600 Update Manager application.

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

No, Hitachi Energy received information about this vulnerability through responsible disclosure.

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.

Acknowledgement

Hitachi Energy thanks the following for working with us to help protect customers:

- May Chaffin, U.S. Department of Energy – Idaho National Lab - CyTRICS researcher.

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
2021-10-26	A	Initial public release.