REVISION: 1
PUBLICATION DATE: 2022-10-13
DOC. IDENTIFIER: 8DBD000102
PUBLISHER: HITACHI ENERGY PSIRT
DOCUMENT STATUS: FINAL

HITACHI
Inspire the Next

CYBERSECURITY ADVISORY

PostgreSQL Related Vulnerabilities in Hitachi Energy MicroSCADA X DMS600 Product

CVE-2021-32027
CVE-2021-32028

Notice

Hitachi Energy

Summary

Hitachi Energy is aware of a report of vulnerabilities in PostgreSQL that is used in the DMS600 product version listed in this document. Remediated version is available that remediates the identified vulnerabilities.

An attacker who successfully exploited the vulnerabilities could gain unauthorized access to information.

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-2021-32027 CVSS v3.1 Base Score: 8.8 High CVSS v3.1 Vector: /AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H Link to NVD: click here	A vulnerability exists in the affected version of PostgreSQL, where while modifying certain SQL array values, missing bounds checks let authenticated database users write arbitrary bytes to a wide area of server memory. Successful exploitation may cause unauthenticated user to gain access to the data, causing confidentiality and integrity issue.
CVE-2021-32028 CVSS v3.1 Base Score: 6.5 Medium CVSS v3.1 Vector: /AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N Link to NVD: click here	A vulnerability exists in the affected version of PostgreSQL, where when using an INSERT ... ON CONFLICT ... DO UPDATE command on a purpose-crafted table, an authenticated database user could read arbitrary bytes of server memory.

Affected Product Versions & Recommended Immediate Actions

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

Affected Version	Recommended Actions
DMS600 4.5	The vulnerabilities are remediated in DMS600 4.6. Please upgrade to at least DMS600 version 4.6 or apply general mitigation factors

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

General Mitigation Factors/Workarounds

Note that in DMS600, PostgreSQL is deployed and accessible only from localhost. Remote connections are not allowed by default.

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.

We recommend following the cybersecurity deployment guideline as follows:

1MRK511518 MicroSCADA X Cyber Security Deployment Guideline

Frequently Asked Questions

What is DMS600?

DMS600 is a modern Distribution Management System (DMS) functionality tightly integrated with SCADA system that enables new real-time applications for improved network monitoring and outage management.

What might an attacker use the vulnerability to do?

An attacker who successfully exploited this vulnerability could access to information without proper access rights.

How could an attacker exploit the vulnerability?

An attacker could exploit the vulnerability by gaining access to the computer where DMS600 is installed. Additionally, the attacker needs to have an access as well to the PostgreSQL to launch a custom SQL command. Recommended practices help to mitigate such attacks, see section Mitigating Factors above.

Could the vulnerability be exploited remotely?

PostgreSQL is deployed and accessible only from localhost. Remote connections are not allowed by default. Firewall should also block all connections to the port TCP/5432.

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, at the date of this advisory publication Hitachi Energy had not received any information indicating that this vulnerability had been exploited.

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
2022-10-13	1	Initial public release.

DocuSigned by: