TLP:CLEAR
REVISION: 1
PUBLICATION DATE: 2023-03-28
DOC. IDENTIFIER: 8DBD000138
PUBLISHER: HITACHI ENERGY PSIRT
DOCUMENT STATUS: FINAL

HITACHI
Inspire the Next

CYBERSECURITY ADVISORY

Multiple Vulnerabilities in Hitachi Energy's MicroSCADA System Data Manager SDM600 Product

CVE-2022-3682
CVE-2022-3683
CVE-2022-3684
CVE-2022-3685
CVE-2022-3686

Notice

Hitachi Energy

Summary

Hitachi Energy is aware of a private report of multiple vulnerabilities in the MicroSCADA System Data Manager SDM600 versions listed below. An update is available that resolves the vulnerabilities. Please refer to the Recommended Immediate Sections for remediation and mitigation strategy.

An attacker who successfully exploited this vulnerability could take remote control of the product.

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-2022-3682 CVSS v3.1 Base Score: 9.9 Critical CVSS v3.1 Vector: AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H Link to NVD: click here CWE: 434 - Unrestricted Upload of File with Dangerous Type	A vulnerability exists in the SDM600 file permission validation. An attacker could exploit the vulnerability by gaining access to the system and uploading a specially crafted message to the system node, which could result in Arbitrary code Executing.
CVE-2022-3683 CVSS v3.1 Base Score: 7.7 High CVSS v3.1 Vector: AV:N/AC:L/PR:L/UI:N/S:C/C:N/I:H/A:N Link to NVD: click here CWE-285: Improper Authorization	A vulnerability exists in the SDM600 API web services authorization validation implementation. An attacker who successfully exploits the vulnerability could read data directly from a data store that is not restricted, or insufficiently protected, having access to sensitive data.
CVE-2022-3684 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 CWE-404: Improper Resource Shutdown or Release	A vulnerability exists in a SDM600 endpoint. An attacker could exploit this vulnerability by running multiple parallel requests, the SDM600 web services become busy rendering the application unresponsive.
CVE-2022-3685 CVSS v3.1 Base Score: 7.5 High CVSS v3.1 Vector: AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H Link to NVD: click here CWE-269: Improper Privilege Management	A vulnerability exists in the SDM600 software. The software operates at a privilege level that is higher than the minimum level required. An attacker who successfully exploits this vulnerability can escalate privileges.
CVE-2022-3686 CVSS v3.1 Base Score: 4.8 Medium CVSS v3.1 Vector: AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:L Link to NVD: click here CWE-285: Improper Authorization	A vulnerability exists in the SDM600 API permission check mechanism. Successful exploitation may cause unauthenticated user to gain access to device data, causing confidentiality and integrity issues.

Affected Products and Recommended Immediate Actions

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

CVE versions	Affected Version	Recommended Actions
CVE-2022-3682 CVE-2022-3683 CVE-2022-3684 CVE-2022-3686	All SDM600 versions prior to version 1.2 FP3 HF4 (Build Nr. 1.2.23000.291)	The vulnerabilities are remediated in SDM600 1.3.0.1339. Please update to SDM600 1.3.0.1339 version or apply mitigation as described in the Mitigation Factors/Workarounds Section.
CVE-2022-3685	All SDM600 versions prior to version 1.3.0 (Build Nr. 1.3.0.1339)	Apply mitigation as described in the Mitigation Factors/Workarounds Section.

Mitigation Factors/Workarounds

It is recommended to implement and continuously revise least privileges principles to minimize permissions and accesses to SDM600 related resources. Furthermore, recommended security practices as defined in SDM600 security deployment guideline and firewall configurations can help to 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 System Data Manager (SDM600)?

SDM600 (System Data Manager) is a comprehensive software solution for automatic management of service and cyber security relevant data across your substations. SDM600 is based on flexible and remotely accessible system architecture. It provides you with efficient data and user management of all stations from one central point.

How could an attacker exploit the vulnerability?

To exploit the disclosed vulnerabilities the attacker must gain access to the 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 Mitigation Factors above.

Could the vulnerability be exploited remotely?

Yes, an authenticated attacker who has network access to an affected system node could exploit these vulnerabilities. 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?

No, Hitachi Energy received information about these vulnerability through internal finding.

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

This advisory will be updated as new relevant information becomes available. Please subscribe to Hitachi Energy's Cybersecurity Alerts & Notifications to get notified:

https://www.hitachienergy.com/offering/solutions/cybersecurity/alerts-and-notifications/subscribe

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
2023-03-28 Same as document publication date	1	Initial public release.

DocuSigned by: