REVISION: A
PUBLICATION DATE: 2021-08-31
DOC. NUMBER: 9AKK107992A4700
PUBLISHER: HITACHI ABB POWER GRIDS PSIRT

CYBERSECURITY ADVISORY

Storage of Sensitive Information Vulnerability in Hitachi ABB Power Grids System Data Manager – SDM600 Product

CVE-2021-35526

Notice

Affected Products and Versions

All System Data Manager – SDM600 versions prior to version 1.2 FP2 HF6 (Build Nr. 1.2.14002.257)

Vulnerability ID

CVE ID: CVE-2021-35526

Summary

An update is available that resolves a privately reported backup file without encryption vulnerability in the System Data Manager – SDM600 product versions listed above. An attacker who successfully exploited this vulnerability could gain access to sensitive information.

Vulnerability Severity and Details

The severity assessment has been performed by using the FIRST Common Vulnerability Scoring System (CVSS) v3.1. The CVSS Environmental Score, which can affect the vulnerability severity, is not provided in this advisory since it reflects the potential impact of a vulnerability within the end-user organizations' computing environment; end-user organizations are therefore recommended to analyze their situation and specify the Environmental Score.

CVE ID	Detail Description
CVE-2021-35526 CVSS v3.1 Base Score: 6.3 Medium CVSS v3.1 Temporal Score: 5.8 CVSS v3.1 Vector: AV:L/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:L/E:H/RL:O/RC:R Link to NVD: click here CWE: CWE-312 Cleartext Storage of Sensitive Information	The vulnerability exists due to application does not encrypt backup files. A local operating system level user with access to the system can modify backup files and might allow local users to overwrite system configuration files and gain privileges.

Recommended Immediate Actions

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

Affected Version	Recommended Actions
All SDM600 versions prior to version 1.2 FP2 HF6 (Build Nr. 1.2.14002.257)	The problem is remediated as of the following product version SDM600 version 1.2 FP2 HF6 (Build Nr. 1.2.14002.257). Hitachi ABB Power Grids recommends that customers apply the update at the earliest convenience. After successful upgrade it is recommended to move previously created vulnerable backups to secure place to avoid any non-authorized access.

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.

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 the scope of the vulnerability?

An attacker who successfully exploited this SDM600 backup vulnerability could access potential sensitive files and gathering configuration related data which could be useful for further tailored attack.

What is the SDM600 application?

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.

What might an attacker use the vulnerability to do?

As the backup information is stored in cleartext (included encoded information), attackers could potentially read it. Malicious attacker could reuse potential sensitive configuration data for further tailored attacks.

Could the vulnerability be exploited remotely?

No, this vulnerability can only be exploited locally. The attacker needs to have authentication credentials and successfully authenticate on the system.

What does the update do?

The update removes the vulnerability by implementing encryption on backup file.

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

No, Hitachi ABB Power Grids received information about this vulnerability through responsible disclosure.

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

No. We are not aware of malware exploiting this vulnerability.

References

1. SDM600 v1.2 Cumulative release notes - https://search.abb.com/library/Download.aspx?DocumentID=3VAC000189&LanguageCode=en&DocumentPartId=&Action=Launch

Support

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

Revision

Date of the Revision	Revision	Description
2021-08-31	A	Initial public release.