CYBER SECURITY ADVISORY

Vulnerabilities in Telephone Gateway TG/S 3.2

ABBVU-ELSB-R-6530

Notice

The information in this document is subject to change without notice, and should not be construed as a commitment by ABB.

ABB 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 ABB 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 ABB 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 ABB, 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.

Affected Products

TG/S 3.2 Telephone Gateway, Analogue, MDRC
Order code: 2CDG 110 135 R0011

6186/11 Telefon-Gateway, Analog (Busch-Jaeger brand)
Order code: 2CKA006136A0187

The product sends configurable voice messages via the telephone network. Apart from the voice messages, e-mail or SMS messages can be sent. Commands via DTMF/MFV can be executed.

Vulnerability ID

ABBVU-EPBP-R-6530

Summary

ABB is privately informed about vulnerabilities in the product listed in section Affected Products.

An attacker who has access to the product via a LAN network can take over control over the product and might re-configure it accordingly. It is therefore recommended to do any re-configuration of the product only in a point to point connection between a trusted, secure computer and the device. The computer shall be disconnected from the internet during the time of re-configuration. If the above explained mitigations are implemented, the device can remain in operation as the reported vulnerabilities are limited to the integrated web browser.

The product has already been **phased out in 2015** and has reached obsolete status. The latest release available is **version 0.1.41** dated from **09/2011**. At the moment there are no plans of corrective measures for this specific issue in the affected products.

More information can be found on the product web page:

https://new.abb.com/products/2CDG110135R0011/tg-s3-2-telephone-gateway-analogue-mdrc

Vulnerability Severity

The severity assessment has been performed by using the FIRST Common Vulnerability Scoring System (CVSS) v3. 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.

Vulnerability	Base Score	Temporal Score	Scoring Link	CVE-ID
CWE-287: Improper Authentication and Access Control	9.1	8.0	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N/E:P/RL:W/RC:R	CVE-2019-19104
CWE-256: Unprotected Storage of Credentials	6.2	5.5	CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N/E:P/RL:W/RC:R	CVE-2019-19105
CWE-264: Permissions, Privileges, and Access Controls	9.1	8.0	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N/E:P/RL:W/RC:R	CVE-2019-19106
CWE-200: Information Exposure	6.2	5.5	CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N/E:P/RL:W/RC:R	CVE-2019-19107

Recommended immediate actions

The vulnerabilities listed in section Vulnerability Severity are concerning the internal web server of the device. The internal web server is primarily used for the configuration of the device. It is not required for its normal operation. Therefore, it is recommended to configure the device via web browser only within a secured network environment. At best is to establish a point-to-point connection between a computer that runs the web client and the IoT device.

The above suggested mitigation shall ensure that physical access to the IoT device is only possible for trusted personal.

Vulnerability Details

The product referenced in Affected Products is subject to four vulnerabilities as listed below in this section.

CWE-287: Improper Authentication and Access Control

By accessing a specific uniform resource locator (URL) on the product integrated web server, a malicious user is able to access different endpoints of the application without authenticating, which violates of the access-control (ACL) rules.

This issue allows obtaining sensitive information that may aid in further attacks and privilege escalation.

CWE-256: Unprotected Storage of Credentials

The backup function saves the current settings and configuration of the application in the backup.tgz file, this file stores the credentials of the existing user accounts and other configuration's credentials in plaintext.

CWE-264: Permissions, Privileges, and Access Controls

The application does not employ proper access-control (ACL) rules at many endpoints, namely when one tries to review or edit the existing data that should be restricted to rules. Based on the lack of properly implemented ACL, a malicious user, for example, can take advantage of the functions linked to the viewing or changing user profiles page.

Note that this issues also lets edit user’s profiles and applications settings without actually having the permission to do so.

CWE-200: Information Exposure

The "Configuration" pages of the user profiles and "Services" contains the password in plaintext; the contents of the sensitive fields are hidden on the pages via "password" field attribute, this approach cannot be deemed as permissible from a security point of view since it does not protect data itself.

Mitigating Factors

To mitigate any risk that is resulting from the vulnerabilities described in this document, it is recommended to disconnect the device from any TCP/IP network. If configuration changes are required, it is to be ensured that only trusted personnel can physically access the device and create a Point-to-Point connection with a computer running a WEB browser as a client and the IoT device as the server. This way it is ensured that malicious users cannot access the device from remote.

Once the device is configured according to its technical manual and disconnected from any TCP/IP network, a normal operation is seen without risk.

The device shall not be connected to a network that has Internet access.

Impact of workaround

As the manual states, device shall not be directly connected to the Internet (any untrusted network). The workarounds described in section Mitigating Factors, result into the inconvenience that a reconfiguration of the device shall only be done when accessing the TCP/IP Port of the device on a Point-to-Point basis.

Frequently Asked Questions

What is the scope of the vulnerability?

An attacker who successfully exploited one or more of the vulnerabilities listed in section Vulnerability Details may:

- take over control of the device.
- get access to user information such as but not limited to phone numbers and other configuration details and personal information.
- set the device out of operation and confront the user with a denial of service.

What causes the vulnerability?

The vulnerability is caused by a vulnerable, integrated WEB Server allowing to configure the IoT device. For details please see section: Vulnerability Details.

What is the component?

The effected component inside the IoT device is the integrated WEB Server.

What might an attacker use the vulnerability to do?

An attacker who successfully exploited this vulnerability could cause the affected system to:

- operate in an unintended way e.g. call wrong or no phone number at all.
- call a phone number to play an audio file defined by the malicious user.
- whatever the malicious user configures it to do as if it was a legitimate user.

How could an attacker exploit the vulnerability?

An attacker could try to exploit the vulnerability by creating a specially crafted message and sending the message to the IoT device. It is therefore recommended to avoid connecting the device to a TCP/IP network as described in section: Mitigating Factors.

Could the vulnerability be exploited remotely?

Yes, if the IoT device is connected to a network where an attacker has access to. It is therefore recommended to follow the actions described in section: Mitigating Factors.

Why is there no SW Update available for the device that fixes the known vulnerabilities?

At the moment there are no plans of corrective measures for this specific issue in the affected products

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

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

When this security advisory was issued, had ABB received any reports that this vulnerability was being exploited?

No, ABB had not received any information indicating that this vulnerability had been exploited when this security advisory was originally issued.

Acknowledgements

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

Maxim Rupp, Security Researcher & Consultant

Support

For additional information and support please contact your local ABB service organization. For contact information, see https://new.abb.com/contact-centers.

Information about ABB's cyber security program and capabilities can be found at www.abb.com/cybersecurity.