Weak Database Encryption Vulnerability in Relion® 630 series version 1.3 and earlier releases

ABBVU-EPDS-DR1605

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

Relion® 630 series 1.1, 1.1.0.C1 or earlier
Relion® 630 series 1.2, 1.2.0.B4 or earlier
Relion® 630 series 1.3, 1.3.0.A7 or earlier

Vulnerability ID

ABB ID: ABBVU-EPDS-DR1605

Summary

A privately reported vulnerability in weak database encryption is in the product versions listed above.

An attacker who successfully exploited this vulnerability could delete or modify the database. Removing or modifying the database will make the device inoperable. The database contains cross reference data for faster indexing and searching.

The database does not contain any secret information.

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

Vulnerability Severity

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

CVSS v3 Base Score:	4.2 (Medium)
CVSS v3 Temporal Score:	4.0 (Medium)
CVSS v3 Vector:	AV:A/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H/E:P/RL:U/RC:C
CVSS v3 Link:	https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=AV:A/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H/E:P/RL:U/RC:C

Corrective Action or Resolution

No updates exist for fixing the vulnerability. At the moment there are no plans of corrective measures for this specific issue in the affected products.

The latest releases available are:

- 630 series 1.1 - 1.1.0.C1
- 630 series 1.2 - 1.2.0.B4
- 630 series 1.3 - 1.3.0.A7

Vulnerability Details

A vulnerability exists in the key generation for the encryption key that is used to encrypt a device database. The database does not contain any secret information. The database contains cross reference data for faster indexing and searching.

Removing or modifying the database will make the device inoperable.

Mitigating Factors

Recommended security practices and firewall configurations (including VPN) 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/services 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.

Workarounds

None exists.

Frequently asked questions

What is the scope of the vulnerability?

An attacker who successfully exploited this vulnerability could delete or modify the internal database on the device. The information stored in the database consists of indexing data for faster searching.

What causes the vulnerability?

The vulnerability is caused by using a predictable key generation for encryption key used to encrypt the database.

What is the database in the device?

The database contains cross reference data for faster indexing and searching.

What might an attacker use the vulnerability to do?

An attacker who successfully exploited this vulnerability could delete or modify the database making the device inoperative.

How could an attacker exploit the vulnerability?
In order for the attacker to try to exploit the vulnerability, local file access is needed for the affected device. This would require that the attacker has access to the system 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 Mitigating Factors above.

Could the vulnerability be exploited remotely?
Yes, an attacker who has network access to an affected system node could exploit this vulnerability. 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/services exposed.

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:

- Aleksandr Tlyapov (Kaspersky Lab) for discovering this vulnerability.

Support

For additional information and support please contact your local ABB service organization. For contact information, see www.abb.com.

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