SSA-042050: Know-How Protection Mechanism Failure in TIA Portal

Publication Date:	2023-06-13
Last Update:	2023-12-12
Current Version:	V1.1
CVSS v3.1 Base Score:	6.2

SUMMARY

The know-how protection feature in Totally Integrated Automation Portal (TIA Portal) does not properly update the encryption of existing program blocks when a project file is updated. This could allow attackers with access to the project file to recover previous - yet unprotected - versions of the project without the knowledge of the know-how protection password.

Siemens is preparing fix versions and recommends countermeasures for products where fixes are not, or not yet available.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
Totally Integrated Automation Portal (TIA Portal) V14: All versions	Currently no fix is planned Archive the project: the optimization of project data during archiving removes older, possibly unprotected project content; see also the chapter “Protecting Blocks” in the system manual (https://support.industry.siemens.com/cs/mdm/109742284?c=87347935883)
Totally Integrated Automation Portal (TIA Portal) V15: All versions	Currently no fix is planned Archive the project: the optimization of project data during archiving removes older, possibly unprotected project content; see also the chapter “Protecting Blocks” in the system manual (https://support.industry.siemens.com/cs/mdm/109764516?c=105012867723)
Totally Integrated Automation Portal (TIA Portal) V15.1: All versions	Currently no fix is planned Archive the project: the optimization of project data during archiving removes older, possibly unprotected project content; see also the chapter “Protecting Blocks” in the system manual (https://support.industry.siemens.com/cs/mdm/109755202?c=105012867723)
Totally Integrated Automation Portal (TIA Portal) V16: All versions	Currently no fix is planned Archive the project: the optimization of project data during archiving removes older, possibly unprotected project content; see also the chapter “Protecting Blocks” in the system manual (https://support.industry.siemens.com/cs/mdm/109773506?c=126979557387)

Totally Integrated Automation Portal (TIA Portal) V17: All versions	Currently no fix is planned Archive the project: the optimization of project data during archiving removes older, possibly unprotected project content; see also the chapter "Protecting Blocks" in the system manual (https://support.industry.siemens.com/cs/mdm/109798671?c=132780438283)
Totally Integrated Automation Portal (TIA Portal) V18: All versions	Currently no fix is planned Archive the project: the optimization of project data during archiving removes older, possibly unprotected project content; see also the chapter "Protecting Blocks" in the system manual (https://support.industry.siemens.com/cs/mdm/109815056?c=132780438283)
Totally Integrated Automation Portal (TIA Portal) V19: All versions	Currently no fix is available Archive the project: the optimization of project data during archiving removes older, possibly unprotected project content; see also the chapter "Protecting Blocks" in the system manual (https://support.industry.siemens.com/cs/mdm/109815056?c=132780438283)

WORKAROUNDS AND MITIGATIONS

Product-specific remediations or mitigations can be found in the section Affected Products and Solution.
Please follow the General Security Recommendations.

GENERAL SECURITY RECOMMENDATIONS

As a general security measure, Siemens strongly recommends to protect network access to devices with appropriate mechanisms. In order to operate the devices in a protected IT environment, Siemens recommends to configure the environment according to Siemens' operational guidelines for Industrial Security (Download: https://www.siemens.com/cert/operational-guidelines-industrial-security), and to follow the recommendations in the product manuals. Additional information on Industrial Security by Siemens can be found at: https://www.siemens.com/industrialsecurity

PRODUCT DESCRIPTION

Totally Integrated Automation Portal (TIA Portal) is a PC software that provides access to the complete range of Siemens digitalized automation services, from digital planning and integrated engineering to transparent operation.

VULNERABILITY CLASSIFICATION

The vulnerability classification has been performed by using the CVSS scoring system in version 3.1 (CVSS v3.1) (https://www.first.org/cvss/). The CVSS environmental score is specific to the customer's environment and will impact the overall CVSS score. The environmental score should therefore be individually defined by the customer to accomplish final scoring.

An additional classification has been performed using the CWE classification, a community-developed list of common software security weaknesses. This serves as a common language and as a baseline for weakness identification, mitigation, and prevention efforts. A detailed list of CWE classes can be found at: https://cwe.mitre.org/.

Vulnerability CVE-2023-30757

The know-how protection feature in affected products does not properly update the encryption of existing program blocks when a project file is updated.

This could allow attackers with access to the project file to recover previous - yet unprotected - versions of the project without the knowledge of the know-how protection password.

CVSS v3.1 Base Score	6.2
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N/E:P/RL:T/RC:C
CWE	CWE-693: Protection Mechanism Failure

ACKNOWLEDGMENTS

Siemens thanks the following party for its efforts:

- Eli Biham, Sara Bitan, Alon Dankner, Arnon Lazerson, and Assaf Rosenbaum from Faculty of Computer Science, Technion Haifa for reporting the vulnerability

ADDITIONAL INFORMATION

The related security note can be found in the TIA Portal system manual (V18, chapter 2.2: https://support.industry.siemens.com/cs/ww/en/view/109815056)

For further inquiries on security vulnerabilities in Siemens products and solutions, please contact the Siemens ProductCERT:

https://www.siemens.com/cert/advisories

HISTORY DATA

V1.0 (2023-06-13):	Publication Date
V1.1 (2023-12-12):	Added Totally Integrated Automation Portal (TIA Portal) V19 as affected product

TERMS OF USE

Siemens Security Advisories are subject to the terms and conditions contained in Siemens' underlying license terms or other applicable agreements previously agreed to with Siemens (hereinafter "License Terms"). To the extent applicable to information, software or documentation made available in or through a Siemens Security Advisory, the Terms of Use of Siemens' Global Website (https://www.siemens.com/terms_of_use, hereinafter "Terms of Use"), in particular Sections 8-10 of the Terms of Use, shall apply additionally. In case of conflicts, the License Terms shall prevail over the Terms of Use.