ABB DOC ID: 2CMT2018-005753
REVISION: B
DATE: 2018-12-21

CYBER SECURITY ADVISORY

# Vulnerability in GATE E2 – Cross-site scripting

## ABBVU-EPPC-3099-SE-003

## 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

ABB GATE-E2, All product versions

ABB GATE-E1, All product versions

# Vulnerability ID

ABB ID: ABBVU-EPPC-3099-SE-003

CVE ID: CVE-2018-18997

# Summary

An attacker who successfully exploited the vulnerability could inject client-side scripts into the product's web pages viewed by other users. This can compromise the browser of a user connecting to the web interface of the product.

The ABB products in scope of this vulnerability advisory will not be updated with new firmware as products are in end-of-life (EOL). Instead the customers who have purchased the affected products have received an email with instructions how to secure an installation. Customers are strongly recommended to apply the proposed mitigations to minimize the risk that the privately reported vulnerability is exploited.

# 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.

CVSS v3 Base Score: 7.1 (High)

CVSS v3 Temporal Score: 6.9 (Medium)

CVSS v3 Vector: AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:L/E:F/RL:U/RC:C

CVSS v3 Link:

https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:L/E:F/RL:U/RC:C

NVD Summary Link:

https://nvd.nist.gov/cvss/v3-calculator?vector=AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:L/E:F/RL:U/RC:C

# Recommended immediate actions

ABB advises customers to promptly follow the recommendations in the Mitigating Factors section.

# Vulnerability Details

An attacker can use cross-scripting (XSS) attack to inject malicious scripts into affected products web pages. User interaction is required for a successful exploitation, because user must be connected to web interface in order for the exploitation to succeed.

# Mitigating Factors

Recommended security practices and firewall configurations 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 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 the scope of the vulnerability?

An attacker who successfully exploited this vulnerability could inject client-side scripts into web pages viewed by other users.

## What causes the vulnerability?

The vulnerability is caused by the lack of proper output encoding in the web application of the affected product.

## What is the affected product?

All product versions of GATE-E2 and GATE-E1 are affected.

## What might an attacker use the vulnerability to do?

An attacker who successfully exploited this vulnerability could run arbitrary code in a user's browser visiting the system nodes web portal. This may allow attacker to compromise further assets.

## How could an attacker exploit the vulnerability?

An attacker could try to exploit the vulnerability by connecting to the affected system node authentication interface and launch a cross-scripting attack. 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 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:

Nelson Berg (Applied Risk) for providing vulnerability details and proof of concept.

## 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.