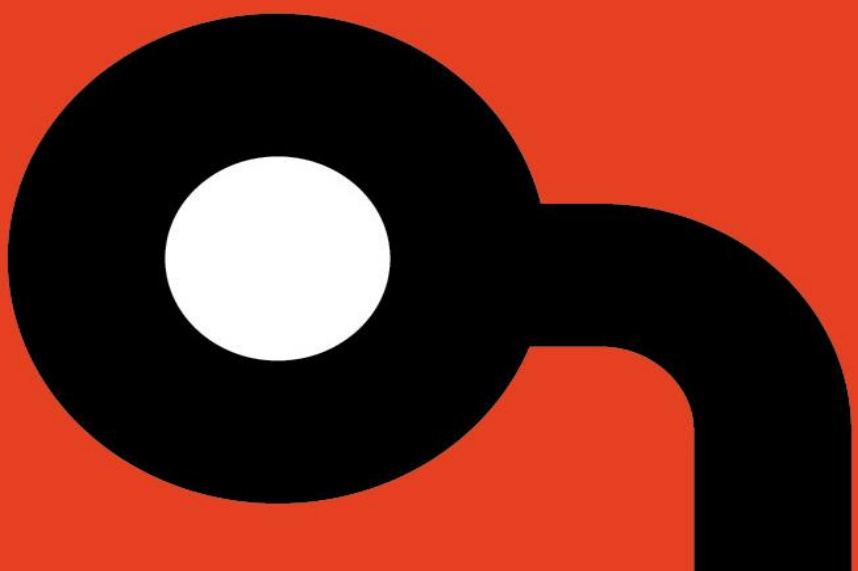
Applied Risk

AR2018008

ABB GATE E1/E2 Multiple vulnerabilities

Author: Nelson Berg

Release Date: December 17, 2018



Copyright Notices

OVERVIEW

Two vulnerabilities were found in the ABB GATE E1/E2 devices. These findings include a total lack of authentication for the administrative interfaces on the device, as well as an unauthenticated persistent Cross-Site Scripting vulnerability. As a result of these findings, ABB has put the GATE-E2 in End-of-Life. The E1 device was already in EoL.

AFFECTED PRODUCTS

ABB GATE-E2, All product versions

ABB GATE-E1, All product versions

IMPACT

Because no authentication functionality is implemented on any administrative interface, attackers are able to compromise the availability of the device, by continuously resetting the device and the integrity/confidentiality of the device, by modifying/reading registers and allowing for the change of configuration such as the device's IP address.

By inserting a HTML/JavaScript payload in any of the device's properties which are displayed (such as the description or PNIO Device name) it is possible to display/execute HTML/JavaScript in the browser of visitors. Given the context of the device, this will most commonly be the plant operators.

BACKGROUND

Pluto Gateway is a unit providing two-way communication between a Pluto Safety PLC and other field buses. The Pluto Gateway is a compact unit mounted on a DIN rail and can be connected anywhere in a Pluto Safety Bus. The unit has a common interface with Pluto, i.e. the same cabling, and the Pluto Manager PC program can be used for servicing and where necessary programming. Normally, however, all the settings are made via DIP switches, which means that programming tools are not required to put the Gateway itself into operation.

VULNERABILITY DETAILS

Missing Authentication for Critical Functions
The devices do not allow authentication to be configured on its administrative telnet/web interface. Access to the administrative interface allows attackers to compromise the availability of the device, by contiguously resetting the device and the integrity/confidentiality of the device, by modifying/reading registers and allowing for the change of configuration such as the device's IP address.

Applied Risk has calculated a CVSS v3 base score of 9.8 with the vector string AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H for this vulnerability.

Persistent Cross-site scripting
Furthermore, it is possible to inject a HTML/JavaScript payload via both the administrative HTTP and telnet interfaces that will be rendered when viewing the device's web-portal. This can compromise the web browser of an administrator visiting the web-portal.

Applied Risk has calculated a CVSS v3 base score of 7.1 with the vector string AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:L for this vulnerability.

MITIGATION

No official patch has been released for GATE-E1 or Gate-E2 devices.

REFERENCES

Vendor website
https://new.abb.com/

Product page
https://library.e.abb.com/public/6a7784b73eb66879c1257d400029411b/2TLC172009M0210_E.pdf

ABB - Vulnerability in GATE E2 – No Access Control
https://search-ext.abb.com/library/Download.aspx?DocumentID=2CMT2018-005751&LanguageCode=en&DocumentPartId=&Action=Launch

ABB - Vulnerability in GATE E2 – Cross-site scripting
https://search-ext.abb.com/library/Download.aspx?DocumentID=2CMT2018-005753&LanguageCode=en&DocumentPartId=&Action=Launch

NIST - CVE-2018-18995
https://nvd.nist.gov/vuln/detail/CVE-2018-18995

NIST - CVE-2018-18997
https://nvd.nist.gov/vuln/detail/CVE-2018-18997

Common Weakness Enumeration (CWE) definition 306
https://cwe.mitre.org/data/definitions/306.html

Common Weakness Enumeration (CWE) definition 79
https://cwe.mitre.org/data/definitions/79.html

CONTACT DETAILS

For any questions related to this report, please contact Applied Risk Research team at:

Email: research@applied-risk.com

PGP Public Key:

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
mQENBFOgiBQBCACj+Notofe/liuHuc90yy8GAfFn8YFCsMCo7wQmQRNTT43bZQq2
gQr7FTLtOl6rBkOLm8bDk0YY/CtWsjdLh1jlDrWyfU6yIzfcu4CSpn1+5n1ivNN5
17ri+VtmgF392twiKhy2+MC9O4of+GMyu1hy5pIjwi3qGzdNlAnT7m7U/hNzaIR4
ae7+NuWtEvWWKyp3IEEMKTDV/ZOtRD1tfIR8KeBB7Axa8cJdlotw/Ail9TLVB6kt
a/BlvhM/zgWfbEPadnx6B0u7pdW50bTECAs0VHje8mcheTwTCAJo+de3/DqUA34X
oF9aAZWpZWE7VH0O4Q8ZtfrXPFqR2xF8LHhZABEBAAG0REFwcGxpZWQgUmlzayBS
ZXNlYXJjaCBUZWFtIChubyBwYXNzd29yZCkgPHJlc2VhcmNoQGFwcGxpZWQtcmlz
ay5jb20+iQE+BBMBAgAoBQJToIgUAhsjBQkJZgGABgsJCAcDAgYVCAIJCgsEFgID
AQIeAQIXgAAKCRA6nyA79MpeSay8CACSI4UhAget5Z+qEDmz1fe+9krgmx7wwDnF
ig4AVICU8ppJQoUCB5pP6eIV/DM7i+mu8e9zeGlA82t69yTVIANWx72zPmGn5Ku8
4t79gR8V+99PW+O+1rej+96wfL2v+IuOXOcJkTsheUyQZ8Klwc1U8kTdGZEY+/IZ
c32ZhyJ04/cchVP/Zsj2WQIh84wbqa27bTEyyFBnD8FdQ2R4UDTqwACbLgp82m29
P346s80c15RZIX8wUAu0LcNbWJJHRsX6Sa+MozTNug9yWdpZt+nmHEMl95lJYktR
w3+gwyaXeUxALX8Baq2EJDdNx9OlsryiNFdnE9vKIM0+24fTDoqguQENBFOgiBQB
CACtSAm5oBD4kJJY+rtHh6xoytOzP6bFEnrVjqXrXCj+ECG6+N6Droqd072X5hki
qoL1viI4NV+2jrYTtMIu+/nc4zuUFUDRYSm0X/K3WgsqaLA4jdedTm45Tau/Fn6W
26tB5AaddcoDdx6JVGIxFvwU+41KoZ7ouDZo7UEBZ7getPubyR4aPepUsjYnPOUL
0SHH76+b/pC5AZm4crpqWf7Q+qaYQdBIhJbgm5ijFzCyHusYgVGBT1hak81QGpM0
1K9wXki/fJrRyEsWWUjpVSEPRizsFJ60v+NrX50gvvXed8MlX0O9efwgeCmGIVDL
oxF/AmnznYWy0LYWAhh/dW7dABEBAAGJASUEGAECAA8FAlOgiBQCGwwFCQlmAYAA
CgkQOp8gO/TKXkmgdQf/ZtwhL2bs+mlmTUmlT3XO4ekVPRLQKtBYfr8y4rdfnq7Y
MdFYEJAt45R+e4I3I7cIJM1/ImncjFng1EpwFItAXVLa1ktiO6BqT6wBqL6pSBe3
2x5VP8OEnnRubCgYaTotNfiEErgh8cG92tW/TiQArU2dnBcVwYHVwPm450pEv9Aq
BBzgeZ25I1Cv0vlQkQLy9PuTA6DWoxeIxbaMD8ZpKGi+XDrfguJ3tERQMlUA6Fc+
OBkT/NKz8mgecVrwCWbCmScyEhh6onTkevI+mydvsxYG8rE6YVxl3oK5Xi6tvAt9
cUPKKK363nkA1AEoMvTz1bCbmTGvTNWLifoMNtNnGA==
=pAvd
-----END PGP PUBLIC KEY BLOCK-----
```