Security Advisory AR-2016002

MOXA ioLogik Multiple Vulnerabilities

Author: Alexandru Ariciu

Release Date: September 30, 2016

Confidentiality and Copyright Notices

Confidentiality

This document contains confidential information about Applied Risk and their respective businesses, business partners and/or customers, all of which is provided in confidence and may be used by the intended recipient only for the sole purpose of the adjudication of the proposal. It must not be used for any other purpose. Copies of this document may only be provided, and disclosure of the information contained in it may only be made to employees of the intended recipient connected with the negotiations and its named professional advisors who acknowledge its confidential status. Any recipient must not to disclose this information, either wholly or in part, to any other party without prior permission in writing being granted by Applied Risk or any entity controlled by, controlling, or under common control with Applied Risk.

COPYRIGHT NOTICE AND CONFIDENTIALITY STATEMENT

OVERVIEW

Multiple vulnerabilities were found in MOXA E1242 Ethernet remote I/O series used in factory automation. These findings range from code injection in the web application to weak password policies and implementation. There are no known public exploits that target these vulnerabilities.

AFFECTED PRODUCTS

The following products and firmware versions are affected:

- ioLogik E1210
- ioLogik E1211
- ioLogik E1212
- ioLogik E1213
- ioLogik E1214
- ioLogik E1240
- ioLogik E1241
- ioLogik E1242
- ioLogik E1260
- ioLogik E1262

The vulnerabilities have been discovered and validated on MOXA E1242 with firmware version V2.3 Build 15031013.

IMPACT

An authenticated user can inject Javascript in the web pages, thus being able to modify the settings and send bad instrumentation commands to the device. The authentication can be easily bypass because of the weak password policies and their implementation.

BACKGROUND

MOXA is a company specialized in full spectrum products for industrial networking, computing and automation with customers in more than 70 countries. More than 30 million MOXA devices are deployed over the world.

VULNERABILITY DETAILS

Multiple Stored Cross Site Scripting - XSS

It was found that MOXA E1242 web application fails to sanitize user input, resulting in Javascript injection in the webpage. An exploit could allow an attacker to execute arbitrary code in the context of the browser of the users visiting the affected web pages.

An attacker can exploit this by visiting the affected web pages and modifying the parameters that were found to be vulnerable to this attack. The changes to this parameter are permanent, thus any user visiting the infected web page after the attacker will be at risk.

Applied Risk has calculated a CVSSv2 base score of 6.5 for this vulnerability; the CVSS vector string is (AV:N/AC:L/Au:N/C:C/I:C/A:C).

Password sent via HTTP GET method

The md5 hash of the password that is used for authentication on the device is sent as a parameter in each GET request to the server. This is considered to be bad practice, as an attacker with a MITM position can easily circumvent this implementation and bypass the authentication mechanism.

Also, passwords sent via GET are not protected by HTTPS in case that is available, as the password will be found in the GET request which is not encrypted.

Applied Risk has calculated a CVSSv2 base score of 9.0 for this vulnerability; the CVSS vector string is (AV:A/AC:M/Au:N/C:C/I:C/A:C).

Password truncation

The password that is used to authenticate users to the system is truncated to 8 characters. An user trying to use a longer password will have its password cut down to the first 8 characters. Also, the MD5 hash challenge that is created for authentication and is later used in all GET requests will be created using these first 8 characters.

This behavior is considered to be insecure, as it does not provide sufficient protection to the passwords used by the user and also forces the user to use simple passwords that can be easily bypassed.

Applied Risk has calculated a CVSSv2 base score of 9.0 for this vulnerability; the CVSS vector string is (AV:A/AC:M/Au:N/C:C/I:C/A:C)

Missing CSRF Protection

It was discovered during testing that the application lacks CSRF protection mechanisms. An attacker can use this vulnerability to modify the device parameters, settings, restart the device or restore the device to factory settings.

Applied Risk has calculated a CVSS2 base score of 7.5 for this vulnerability; the CVSS vector string is (AV:N/AC:L/Au:N/C:P/I:P/A:P)

MITIGATION

MOXA addressed the reported vulnerabilities by releasing a firmware update for the affected devices. The firmware updates are available at the following link:

http://www.moxa.com/support/sarch_result.aspx?type=soft&prod_id=579&type_id=4

REFERENCES

Vendor website

http://www.moxa.com

Product page

http://www.moxa.com/product/ioLogik_E1242.htm

About Applied Risk

Applied Risk is an established leader in Industrial Control Systems security. We help businesses to protect assets and reduce security risk, providing organisations ranging from Fortune 500 enterprises to small-to-medium sized businesses with the services and solutions they need to transform the way they procure, build, integrate and manage their critical infrastructures. Established in 2012, we have quickly grown to become a major cybersecurity player within the Industrial Automation and Process Control Domain.

For more information, please visit our website at: http://www.applied-risk.com

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-----
```