Applied Risk

Security advisory AR2015001

Multiple vulnerabilities in Moxa industrial managed switches

Author: Erwin Paternotte

Release date: 26/08/2015

Confidentiality statement and copyright notice

Confidentiality statement

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 it's 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

Overview

Applied Risk discovered multiple vulnerabilities in Moxa industrial managed Ethernet switches. These vulnerabilities could be exploited remotely. There are currently no known public exploits specifically targeting these vulnerabilities.

Affected products

The following product lines are affected by the discovered vulnerabilities:

- Moxa EDS-405A/EDS-408A series managed ethernet switches

The vulnerabilities have been discovered and validated on a Moxa EDS-405A switch running firmware version V3.4 build 14031419.

Impact

An authenticated remote attacker could compromise the availability, integrity and confidentiality of a Moxa industrial managed switch, including connected industrial assets.

Background

Moxa is a Taiwan-based company that maintains offices in several countries around the world, including the US, UK, India, Germany, France, China, and Brazil.

The EDS-405A/408A are entry-level 5 and 8-port managed ethernet switches designed especially for industrial applications. The switches support a variety of useful management functions, such as Turbo Ring, Turbo Chain, ring coupling, port-based VLAN, QoS, RMON, bandwidth management, port mirroring, and warning by email or relay.

Vulnerability details

Privilege Escalation

A privilege escalation vulnerability has been found in the administrative web interface of the Moxa industrial ethernet switches. A user level account has by default read only access to the web interface. The check that prevents a user level account from modifying settings in the administrative web interface could be easily circumvented, resulting in elevated access privileges.

Applied Risk has calculated a CVSSv2 base score of 8.5 for this vulnerability; the CVSS vector string is (AV:N/AC:L/Au:S/C:N/I:C/A:C).

Denial of Service

The embedded GoAhead webserver running on the Moxa ethernet switches is vulnerable to a Denial of Service attack. A crafted URL sent by an authenticated user causes a reboot of the device.

Applied Risk has calculated a CVSSv2 base score of 6.8 for this vulnerability; the CVSS vector string is (AV:N/AC:L/Au:S/C:N/I:N/A:C).

Cross-Site Scripting
A Cross-Site Scripting (XSS) vulnerability has been found in the administrative web interface of the Moxa industrial ethernet switches. An input field of the administrative web interface lacks input validation, which could be abused to inject JavaScript code.

Applied Risk has calculated a CVSSv2 base score of 4.3 for this vulnerability; the CVSS vector string is (AV:N/AC:M/Au:N/C:N/I:P/A:N).

Mitigation

Moxa addressed the reported vulnerabilities by releasing a firmware update for the affected devices. The firmware updates are available at the following location on their website:

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

References

Moxa EDS-405A/EDS-408A series ethernet switches

http://www.moxa.com/product/EDS-408405A.htm

OWASP Top 10 2013-A3-Cross-Site Scripting

https://www.owasp.org/index.php/Top_10_2013-A3-Cross-Site_Scripting_%28XSS%29

OWASP Top 10 2013-A7-Missing Function Level Access Control

https://www.owasp.org/index.php/Top_10_2013-A7-Missing_Function_Level_Access_Control

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 advisory, 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-----
```