AR2019001

ControlByWeb X-320M-I Vulnerabilities

Authors: Tom Westenberg, John Elder

Release Date: January 17, 2019

Copyright Notices

COPYRIGHT NOTICE STATEMENT

OVERVIEW

The following vulnerabilities were discovered in ControlByWeb's X-320M-I Web-Enabled Instrumentation-Grade Data Acquisition module 1.05 with firmware revision v1.05;

1. A Denial of Service (DOS) issue was discovered in ControlByWeb's X-320M-I Web-Enabled Instrumentation-Grade Data Acquisition module 1.05 with firmware revision v1.05. An authenticated user can configure invalid network settings, stopping TCP based communications to the device. A physical factory reset is required to restore the device to an operational state. There are no known public exploits which target this vulnerability.
2. A stored cross-site scripting (XSS) issue was discovered in ControlByWeb X-320M-I Web-Enabled Instrumentation-Grade Data Acquisition module 1.05 with firmware revision v1.05. An authenticated user can inject arbitrary script via setup.html in the web interface.

AFFECTED PRODUCTS

ControlByWeb's X-320M-I Web-Enabled Instrumentation-Grade Data Acquisition module;

The following versions are affected:

- Firmware revision v1.05 and prior

IMPACT

Adversaries leveraging these vulnerabilities could cause a DoS condition which renders the device unreachable. A physical factory reset is required to restore the device to an operational state. Alternatively, adversaries could craft scripts to perform malicious actions i.e. redirecting users, attempting to steal data, etc.

BACKGROUND

ControlByWeb produce Ethernet I/O products for web control and monitoring of electrical devices. The X-320 is a web-based instrumentation module that can be used in a variety of scientific and industrial applications such as energy/power monitoring, meteorology and process control.

It has a combination of analog and digital inputs that can be used with the appropriate sensors for measuring voltage, current, temperature, humidity, wind speed, solar radiation, fluid level, flow, frequency, count, etc. Two digital inputs can be user-configured as outputs capable of driving solid state relays or triggering the input of another controller. The X-320 has a built-in web server and all of the data it measures can be viewed using a web browser (or custom computer application).

VULNERABILITY DETAILS

On the /setup.html page, it is possible to cause a denial of service condition by changing 'IP Filter Range 1:' from '255.255.255.255' to '0.0.0.0'. This appears to stop all TCP based communications to the device and a physical factory reset is required to restore the device to an operational state.

CVE-2018-18881 has been assigned to this vulnerability. A CVSS v3 base score of 7.5 has been assigned; the CVSS vector string is (AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H).

A stored cross-site scripting vulnerability exists within the ‘Site Description:’ input on the /setup.html page. Because the input is not sanitised, arbitrary script can be injected and when a user subsequently visits the ‘Status’ page where this input is displayed, the script will be executed.

CVE-2018-18882 has been assigned to this vulnerability. A CVSS v3 base score of 7.6 has been assigned; the CVSS vector string is (AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:H)

MITGATION

ControlByWeb has released a firmware update to address the vulnerabilities found on the X-320M that can be downloaded at: https://www.controlbyweb.com/firmware/X320M V1.06 firmware.zip

Additional ControlByWeb support information can be found at:https://www.controlbyweb.com/support/

REFERENCES

Common Weakness Emuneration (CWE) definition 400
https://cwe.mitre.org/data/definitions/400.html
OWASP Denial of Service
https://www.owasp.org/index.php/Denial_of_Service
OWASP Top 10 (2017)
https://www.owasp.org/index.php/Top_10-2017_Top_10

CONTACT DETAILS

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