Applied Risk

AR2018002

Rockwell Automation Allen-Bradley Safety PLC Denial of Service

Author: Alexey Perepechko

Release Date: June 19, 2018

Copyright Notice

OVERVIEW

A vulnerability in the Rockwell Automation Allen-Bradley CompactLogix 5370 Controller 1769-L30ERMS could allow an unauthenticated, remote threat actor to reboot the device and switch the device to the “Major Non-Recoverable Fault” mode, resulting in a Denial of Service (“DoS”) condition.

AFFECTED PRODUCTS

This vulnerability affects CompactLogix 1769-L30ERMS that are running a firmware release prior to the 30.012 inclusive version.

Only 1769-L30ERMS was confirmed to be affected by this vulnerability. However, all 1769-L30X models and other products from the vendor using Ethernet/IP are potentially affected due to a similar TCP stack code-base.

System administrators can determine which firmware is running from the web-interface of the device or via the Rockwell Automation set of control tools.

IMPACT

An unauthenticated user can craft a malicious ACK TCP packet that will immediately reboot the device. After the reboot, the device enters a “Major Fault” mode which prevents normal operation of the main safety controller program. This mode will not be automatically resolved and requires manual operations to be done by an engineer.

BACKGROUND

The CompactLogix series are used in various sector and industries.

VULNERABILITY DETAILS

The vulnerability is due to incorrect processing of TCP ACK packet additional options by the listener at Ethernet/IP TCP port (default 44818). An incorrect order on the NOP option leads to a immediate device reboot and enters a “Major Fault” mode which must be resolved manually. To trigger the vulnerability, the NOP option must be put first and the number of options must be more than one.

Applied Risk has calculated a score of 7.5 for this vulnerability in CVSSv3 scale. The CVSS vector string is: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

MITIGATION

Rockwell has provided a firmware update addressing the vulnerability. There are no workarounds that address this vulnerability as Ethernet/IP protocol is a main communicative protocol for this device.

REFERENCES

Vendor website:

https://ab.rockwellautomation.com/

Product page:

https://ab.rockwellautomation.com/Programmable-Controllers/CompactLogix-5370-Controllers

CWE-248: Uncaught Exception:

https://cwe.mitre.org/data/definitions/248.html

CVE-ID:

https://nvd.nist.gov/vuln/detail/CVE-2017-9312

CONTACT DETAILS

For any questions related to this report, please contact the 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-----
```