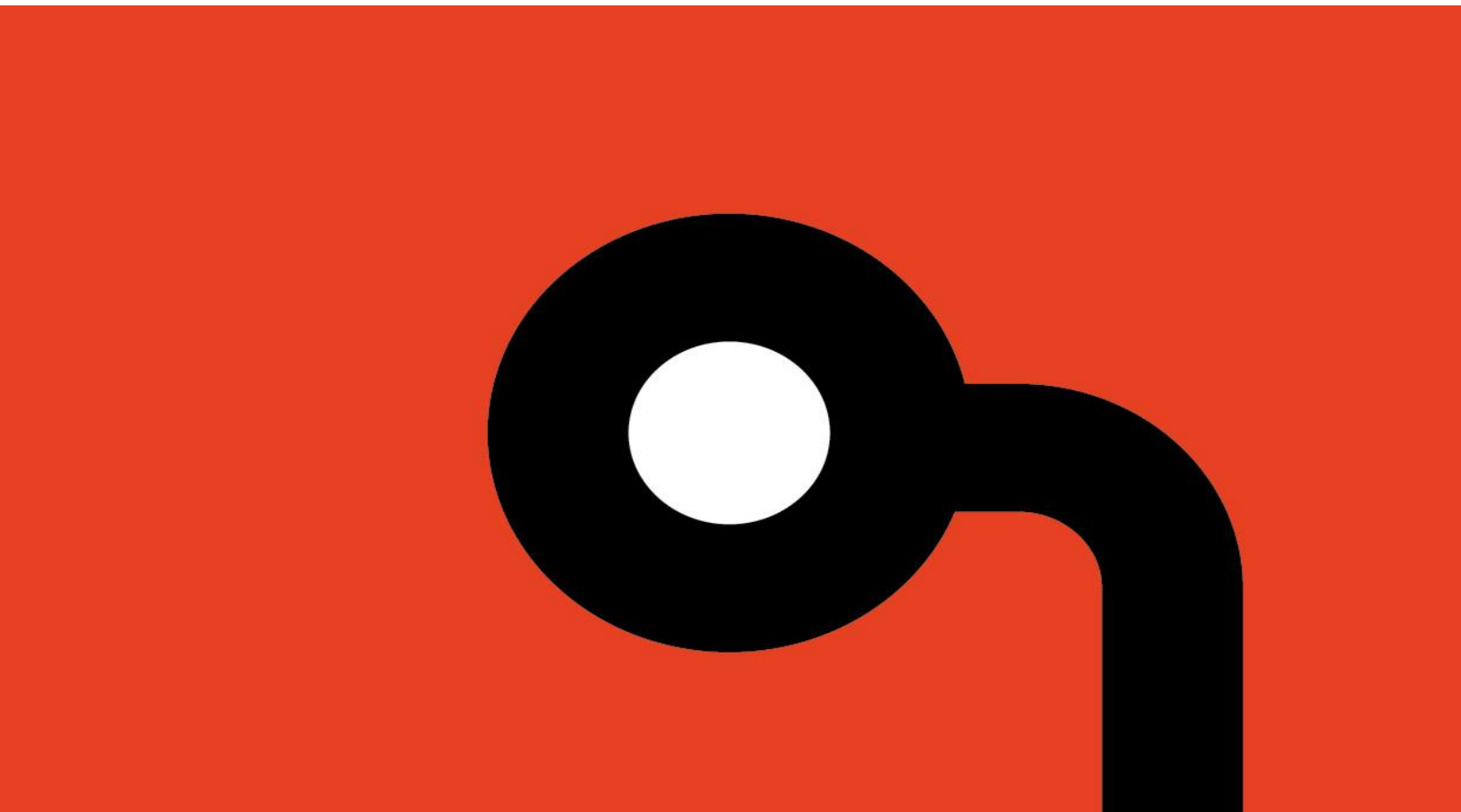
Applied Risk

AR2019004

Rockwell Automation PowerFlex 525 Denial of Service

Author: Nicolas Merle

Release Date: March 28, 2019



OVERVIEW

A denial of service was found in the PowerFlex 525 variable frequency drive used in industrial systems to control the frequency of industrial motors. This finding allows an attacker to crash the Common Industrial Protocol (CIP) in a way that it does not accept any new connection. The current connections however, are kept active, giving attackers complete control over the device. There are no known public exploits that target this vulnerability.

AFFECTED PRODUCTS

Powerflex 525;

The following versions are affected:

- 5.001

The vulnerability has been discovered and validated in the software version 5.001. Older versions are probably affected too.

IMPACT

An unauthenticated user can send a precise sequence of packet effectively crashing the CIP network stack. This creates an error in the control and configuration software which disconnect upon exhausting the connection pool. It is not possible to initiate a new connection to the device after the daemon has crashed, effectively forbidding any legitimate user to recover control. If the attacker maintains the connection used to send the payload open, he can continue sending command as long as the connection is not interrupted. The only way to recover access to the device is to do a power reset.

BACKGROUND

Allen Bradley is a division of Rockwell Automation, which designs and develops industrial devices and software. Such devices are typically found in a variety of industries ranging from manufacturing to the utilities sectors. The impact of exploiting this device in a live production environment could result in the manipulation of physical process and denial of process control.

VULNERABILITY DETAILS

Denial of Service

Applied Risk identified that the PowerFlex 525 is vulnerable to a Denial of Service (DoS). Sending a specific UDP packet, a definite amount of time corrupts the CIP daemon forbidding any new connection to be initiated and disconnecting the configuration and control software from Rockwell Automation.

An attacker can exploit this by sending the sequence after having initiated a CIP session to disconnect all operators and control the process exclusively.

Applied Risk has calculated a CVSSv3 base score of 9.1 for this vulnerability; the CVSS vector string is CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:H.

MITIGATION

Rockwell Automation has developed a patch that mitigates this vulnerability.

TIMELINE

- 30th July 2018: Initial identification of the vulnerability.
- 1st August 2018: Reached to Rockwell Automation for their PGP key.
- 20th August 2018: Follow up for the key.
- 18th September 2018: Final follow up for the key before responsible disclosure.
- 18th September 2018: Rockwell Automation provided a valid PGP key for disclosure.
- 25th September 2018: Disclosure with ICS-CERT of the vulnerability and technical details. PGP keys are shared between members of the Rockwell Automation PSIRT and the Applied Risk team.
- 26th September 2018: Request for technical details and a POC from Rockwell Automation.
- 27th September 2018: Applied Risk sent a POC along with the technical information requested by Rockwell Automation.
- 13th of November 2018: Follow up on the disclosure of the vulnerability by Applied Risk. Rockwell Automation provides update and request some additional information
- 15th of November 2018: Applied Risk provided the necessary information to Rockwell Automation.
- 20th of November 2018: Rockwell Automation set the publication date for the advisory to March 2019
- 28th March 2019: Responsible Disclosure of the vulnerability by Applied Risk in coordination with Rockwell Automation

REFERENCES

Vendor website

https://www.rockwellautomation.com/global/overview.page

Product page

https://ab.rockwellautomation.com/Drives/PowerFlex-525

OWASP

https://www.owasp.org/index.php/Denial_of_Service

CVE-ID: CVE-2018-19282

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-19282

Knowledgebase Raid# 1082684

https://rockwellautomation.custhelp.com/app/answers/detail/a_id/1082684

ICS-Cert Publication

https://ics-cert.us-cert.gov/advisories/ICSA-19-087-01

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-----
```