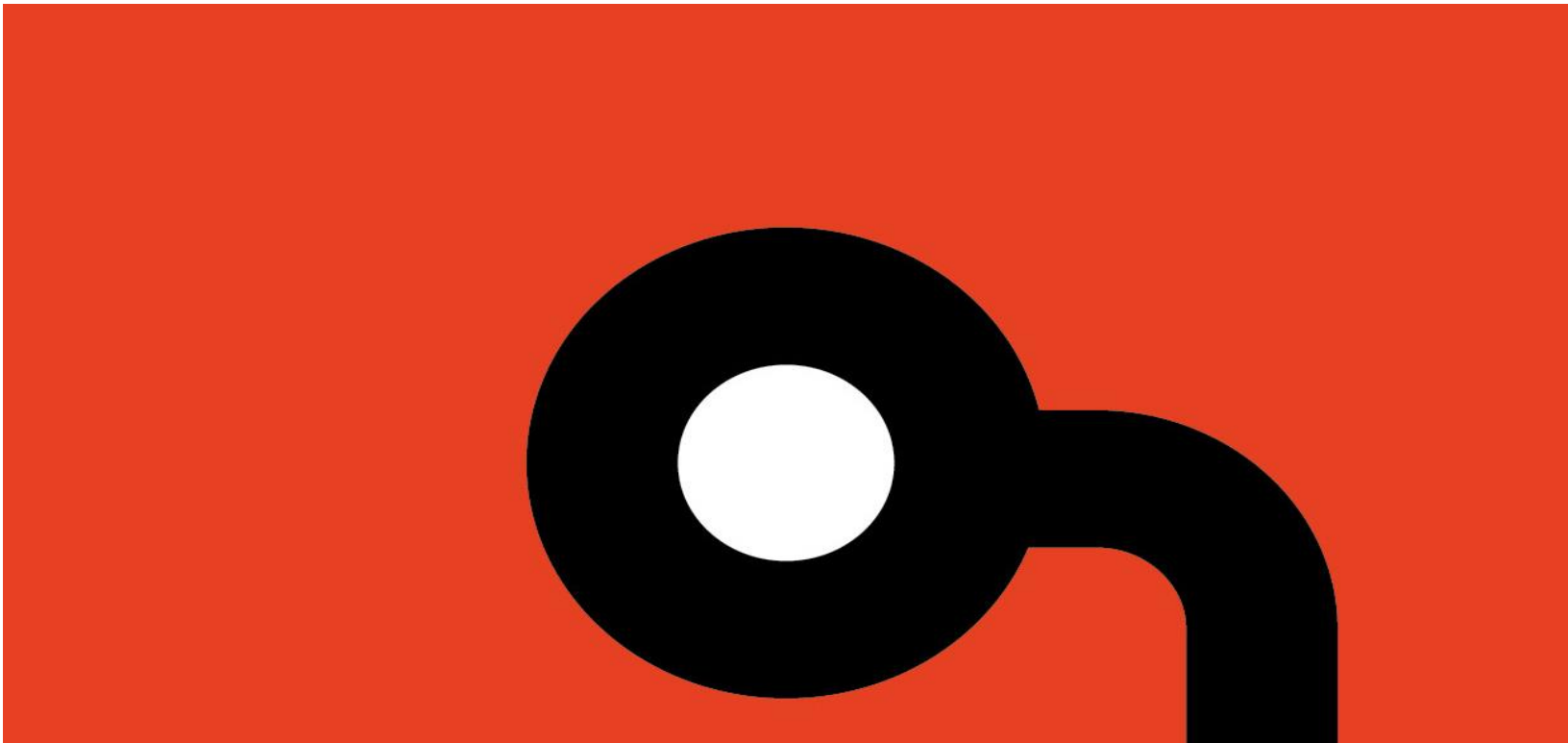

Applied Risk

AR2019003

Triconex TriStation Emulator Denial of Service

Author: Tom Westenberg

Release Date: 19th March 2019

Copyright Notice

OVERVIEW

A vulnerability was identified in Triconex Tristation Emulator's Triconex System Access Application (TSAA) communication stack which causes a Denial of Service (DoS). There are no known public exploits which target this vulnerability.

Schneider Electric indicates this vulnerability does not impact hardware-based controllers.

AFFECTED PRODUCTS

Triconex TriStation 1131 Software Suite;

The following versions are known to be affected:

- Triconex TriStation Emulator version 1.2.0 (installed as part of Triconex TriStation 1131 version 4.9.0)

The vulnerability was discovered and validated using TriStation 1131 v4.9.0 and Triconex TriStation Emulator version 1.2.0. It is unknown – but likely – that older versions of Triconex TriStation Emulator suffer from the same vulnerability.

IMPACT

Adversaries leveraging this vulnerability could cause a DoS of an emulated controller by exploiting the application's TSAA interface.

BACKGROUND

Triconex is a Schneider Electric brand which supplies systems and products in regards to critical control and industrial safety-shutdown technology.

The latest version of the Triconex TriStation Emulator is installed with the TriStation 1131 software. The Triconex TriStation Emulator is software that allows users to emulate and execute TriStation 1131 applications without connecting to a Tricon, Trident, or Tri-GP controller. Using the Emulator, users can test applications in an offline environment, without exposing their online processes to potential application errors.

Schneider Electric Triconex technology is certified by TÜV Rheinland for use in safety applications up to safety integrity level 3 (SIL3), Triconex systems are renowned throughout the world for safety, availability and security.

VULNERABILITY DETAILS

The Emulator application suffers from at least one unique DoS vulnerability. This vulnerability can be triggered by sending a specifically crafted TSAA packet(s) over a network. These packets are sent to the victim using UDP port 1500. Multiple unique packets were identified to cause DoS vulnerabilities.

Communication settings within Triconex TriStation Emulator allow configuration of different Node Numbers. The specifically crafted TSAA packet is required to match the victim's Node Number for successful exploitation.

The vulnerability is likely to be caused through unhandled exceptions in the Triconex TriStation Emulator's TSAA network stack.

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

MITGATION

Schneider Electric indicated a patch shall be released June 2019.

Schneider Electric recommends that its end user always follow the suppliers' guidelines to ensure the security of their installations.

TIMELINE

- 15th July 2018: Initial identification of the vulnerability.
- 16th July 2018: Reached out to Schneider Electric for their PGP key.
- 30th July 2018: Schneider Electric provided a valid PGP key for disclosure. Technical details were shared with Schneider Electric, including the Proof of Concept.
- 2nd August 2018: More information shared with Schneider Electric upon their request.
- 13th August 2018: Asked Schneider Electric on update on their triage efforts. Team is still working on reproducing the issue using the Proof of Concept script.
- 27th August 2018: Schneider Electric indicates they have tested the Proof of Concept on hardware controllers which rejected the Proof of Concept payloads. Schneider Electric indicates the vulnerability only affects the Code Emulator and no hardware components.
- 19th September 2018: Schneider Electric indicates that the outlined vulnerability may not have a planned fixed as the impact is perceived as very low.
- 24th October 2018: Schneider Electric indicates that on 27/9/2018 it was decided that Schneider Electric will address this bug. This fix was scheduled to be released on 1st January 2019.
- 2nd November 2018: CVE-2018-7803 got assigned.
- 18th January 2019: Reached out to Schneider Electric if we can verify the patch before its release on 31st January 2019.
- 22nd January 2019: Schneider Electric indicates that the fix will be delayed.
- 11th March 2019: Applied Risk informs Schneider Electric that it will proceed with the publication of its advisory.
- 14th March 2019: Provided draft advisory to Schneider Electric.
- 19th March 2019: Public disclosure.

REFERENCES

Common Weakness Enumeration (CWE) definition 400
https://cwe.mitre.org/data/definitions/400.html

OWASP Denial of Service
https://www.owasp.org/index.php/Denial_of_Service

CVE-2018-7803
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-7803

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-----
```