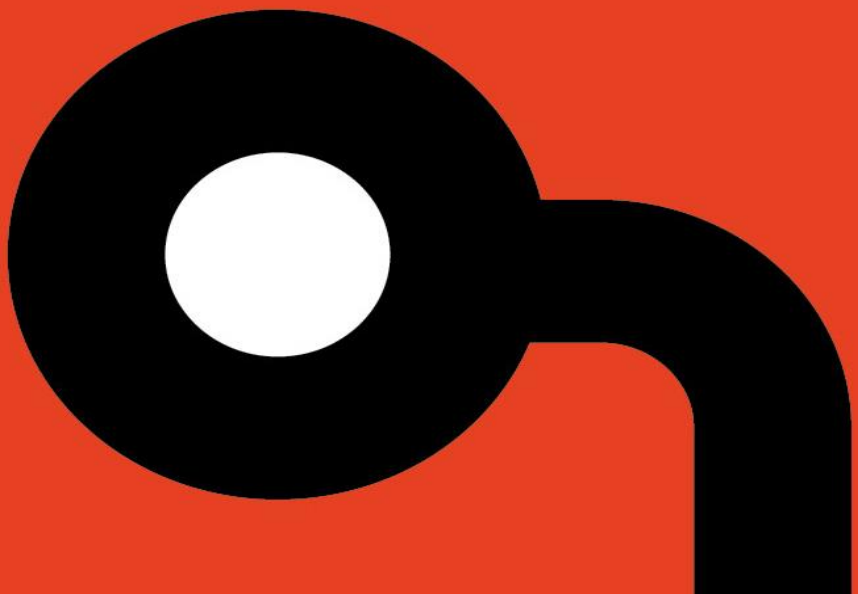
Applied Risk

AR2018007

Pilz PNOZmulti Configurator Cleartext Storage of Sensitive Information

Author: Gjoko Krstic

Release Date: November 30, 2018



Copyright Notice

OVERVIEW

A cleartext storage of sensitive information has been discovered in Pilz PNOZmulti Configurator software that allows a local attacker to read sensitive data in clear-text. There are no known public exploits targeting this vulnerability in said solution.

AFFECTED PRODUCTS

Pilz PNOZmulti Configurator

The following versions are affected:

- Program version: 10.8 and prior

The vulnerability has been discovered and validated on Pilz PNOZmulti Configurator 10.8. Older versions are affected too.

IMPACT

An authenticated user can read credentials stored in clear-text.

BACKGROUND

Pilz GmbH & Co. KG is technology leader in safe automation technology. In this area, Pilz is consistently developing a role as a total solutions supplier with solutions for safety and automation technology. PNOZmulti Configurator - The original tool for your safety circuit configuration. The configuration tool supports you with the project design, configuration, documentation and commissioning of Pilz control systems.

VULNERABILITY DETAILS

Cleartext Storage of Sensitive Information

The vulnerability allows an attacker with access to the PC file system that uses the software PNOZmulti Configurator to read out sensitive data. The data is a configuration data of an HMI device of type PMI m107 diag. The misuse of captured configuration data requires physical access to the PMI m107 diag. It can allow modification of data on affected device once credentials are disclosed.

This issue allows a local authenticated attacker to view credentials in clear-text in an unencrypted configuration file, which is located at:

C:\ProgramData\Pilz\PNOZmulti Configurator v10.8.0\AppData\pmimicroconfig\UserSettings.xml.

Applied Risk has calculated a CVSSv3 score of 4.4 for this vulnerability. The CVSS vector string is CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N.

MITIGATION

Pilz addressed the reported vulnerability by releasing a new version 10.9 for the affected software. The vendor's advisory and software updates are available at the following links:

- https://www.pilz.com/en-GB/support/downloads#currentPage=1&SEARCH=Security%20Advisory&pilz_group_type=download&SORT=dmodified
- https://www.pilz.com/download/restricted/PNOZmulti_Configurator_10_9_0_3000683A41.zip

REFERENCES

Vendor website
https://www.pilz.com

Product page
https://www.pilz.com/en-INT/eshop/00101002067093801Z/PNOZmulti-Configurator-Licence

OWASP
https://www.owasp.org/index.php/Insecure_Storage

Common Weakness Enumeration (CWE) definition 312
https://cwe.mitre.org/data/definitions/312.html

ICS-CERT Advisory (ICSA-19-010-03):
https://ics-cert.us-cert.gov/advisories/ICSA-19-010-03

CVE ID: CVE-2018-19009:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-19009

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-----
```