Applied Risk

AR2019002

Kunbus PR100088 Modbus TCP Gateway Multiple Vulnerabilities

Author: Nicolas Merle

Release Date: February 6, 2019

COPYRIGHT NOTICE

OVERVIEW

Five vulnerabilities were found in the Kunbus PR100088 Modbus gateway used in industrial systems to connect ethernet networks to Modbus networks. These findings include an authentication bypass, password being exchanged over HTTP GET method, an authenticated Denial of Service and an unsafe credential storage vulnerability. There are no known public exploits that target these vulnerabilities.

AFFECTED PRODUCTS

Kunbus PR100088 Modbus gateway;

The following versions are affected:

- 1.0.10232

The vulnerabilities have been discovered and validated in the software version 1.0.10232. Older versions are probably affected too.

IMPACT

An unauthenticated user can change the admin password, use it to get full control of the device, change its configuration and then lock the administrator out. An authenticated user can send a malicious request to the ftp service, stopping the device until the next cold reboot. An attacker able to sniff the traffic would be able to get any password used for login. An unauthenticated user can see and change the Modbus register value via the web interface and reboot the device with a simple command, creating a denial of service. Finally, an attacker could change the Administrator password to the default one, to trick the operator to input back its password that he could in return recover via the ftp service.

BACKGROUND

Kunbus designs and builds industrial device and modules to interconnect network using different types of technologies and protocols. 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 or denial of process control communications.

VULNERABILITY DETAILS

Improper Authentication

Applied Risk identified that the Modbus gateway web application fails to check that the user is logged in when processing the change of password page. This only happens when an admin user logged himself in previously on the device and the device has not been restarted since. The admin password is then modified for the Web server and the FTP server.

An attacker can exploit this by visiting the affected web server and entering a new password value directly via the change password page. If an admin user logged himself during the uptime of the device, the password will be modified. The change of password is permanent, and no reset function is implemented on the device, thus any regular user would not be able to recover access to the device.

Applied Risk has calculated a CVSSv3 base score of 9.6 for this vulnerability; the CVSS vector string is CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H.

Information Exposure Through Query Strings In GET Request

Applied Risk identified that the password that is used for authentication on the device is sent as a parameter in the HTTP GET request used to login. This is considered to be bad practice, as an attacker with a MITM position can easily recover the password.

Also, passwords sent via GET are not protected by HTTPS in case that is available, as the password will be found in the HTTP GET request which is not encrypted.

Applied Risk has calculated a CVSSv3 base score of 8.8 for this vulnerability; the CVSS vector string is CVSS:3.0/AV:A/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H.

Missing Authentication For Critical Function

Applied Risk identified that the registers used to store Modbus values can be read and written to from the web interface without any authentication. This vulnerability also applies to the reset function of the device.

Applied Risk has calculated a CVSSv3 base score of 10.0 for this vulnerability; the CVSS vector string is CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

Improper Input Validation

Applied Risk identified that the FTP service user input is not properly checked. If a request is made with a length greater than 256 characters, the device crashes in such way that a cold-reboot is required.

Applied Risk has calculated a CVSSv3 base score of 4.9 for this vulnerability; the CVSS vector string is CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H

Cleartext Storage of Sensitive Information

Applied Risk identified that the credentials used for the device were stored in clear text in an xml file, which can be retrieved via FTP.

Applied Risk has calculated a CVSSv3 base score of 7.2 for this vulnerability; the CVSS vector string is CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H

MITIGATION

For all issues except Cleartext Storage of Sensitive Information, updating to release R02 of the software will fix the issues according to the vendor. The Cleartext Storage of Sensitive Information issue should be solved in release R03 of the software which is expected to be available at the end of February according to the vendor.

REFERENCES

Vendor website

https://www.kunbus.com/

Product page

https://www.kunbus.com/modbus-tcp-gateway-module.html

Common Weakness Enumeration (CWE) definition 287

https://cwe.mitre.org/data/definitions/287.html

Common Weakness Enumeration (CWE) definition 598

https://cwe.mitre.org/data/definitions/598.html

Common Weakness Enumeration (CWE) definition 306

https://cwe.mitre.org/data/definitions/306.html

Common Weakness Enumeration (CWE) definition 20

https://cwe.mitre.org/data/definitions/20.html

Common Weakness Enumeration (CWE) definition 312

https://cwe.mitre.org/data/definitions/312.html

OWASP

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

ICS-CERT Advisory

https://ics-cert.us-cert.gov/advisories/ICSA-19-036-05

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-----
```