AR2015002

UMG energy and power quality measurement products multiple vulnerabilities

Author: Mattijs van Ommeren

Release Date: October 22, 2015

Confidentiality and Copyright Notices

Confidentiality

This document contains confidential information about Applied Risk and their respective businesses, business partners and/or customers, all of which is provided in confidence and may be used by the intended recipient only for the sole purpose of the adjudication of the proposal. It must not be used for any other purpose. Copies of this document may only be provided, and disclosure of the information contained in it may only be made to employees of the intended recipient connected with the negotiations and its named professional advisors who acknowledge its confidential status. Any recipient must not to disclose this information, either wholly or in part, to any other party without prior permission in writing being granted by Applied Risk or any entity controlled by, controlling, or under common control with Applied Risk.

COPYRIGHT NOTICE AND CONFIDENTIALITY STATEMENT

OVERVIEW

Multiple vulnerabilities were found in Janitza UMG series power and energy quality measurement products. These findings range from information disclosure vulnerabilities to remote code execution by unauthenticated users. There are no known public exploits that target these vulnerabilities.

AFFECTED PRODUCTS

The following products and firmware versions are affected:

- UMG 605 Power Quality Analyser
- UMG 604 Power Analyser
- UMG 512 Power Quality Analyser
- UMG 511 Power Quality Analyser
- UMG 509 Power Quality Analyser
- UMG 508 Multifunction Power Analyser

The vulnerabilities have been discovered and validated on a UMG 604 Power Analyser with firmware version r4051 build 244.

IMPACT

An unauthenticated remote attacker can take full control of the device. By by leveraging the built-in JASIC script language an attacker can adjust system parameters, manipulate measurement values and change the function of the device, compromising availability, integrity and confidentiality of the device itself and dependent systems.

BACKGROUND

Janitza electronics GmbH is a privately owned manufacturer of power factor controllers and energy measurement solutions. Janitza customers include energy supply companies, manufacturers and several industry verticals.

VULNERABILITY DETAILS

Debug interface

The observed device exposes a remote debug interface on TCP port 1239. This allows an unauthenticated remote attacker to read and write arbitrary files including the file that contains the configured passwords.

Applied Risk has calculated a CVSSv2 base score of 10 for this vulnerability; the CVSS vector string is (AV:A/AC:M/Au:N/C:C/I:C/A:C).

Weak password protection

By default the UMG device's web interface is unprotected. A password can be configured, but is limited to a 4-digit value PIN. No controls are in place to prevent PIN guessing, which makes it trivial to guess a valid PIN by trying all possible combinations.

Applied Risk has calculated a CVSSv2 base score of 10 for this vulnerability; the CVSS vector string is (AV:N/AC:L/Au:N/C:C/I:C/A:C).

Default password

The device exposes an FTP and web service used by the GridVis management suite that is protected by a default password. There existed no documented way of changing this password. Once logged an attacker is able to upload and download arbitrary files, including JASIC program logic to modify the device's behavior (e.g. controlling switch outputs).

Applied Risk has calculated a CVSSv2 base score of 10 for this vulnerability; the CVSS vector string is (AV:A/AC:M/Au:N/C:C/I:C/A:C)

Weak session token generation

Session tokens are derived from the 4-digit PIN in combination with a server generated challenge. The challenge suffers from very low entropy. Intercepting an even small sample set of session tokens can potentially result in successful recovery of the PIN due to the limited key space of both the session token and the PIN.

Applied Risk has calculated a CVSSv2 base score of 7.9 for this vulnerability; the CVSS vector string is (AV:A/AC:M/Au:N/C:C/I:C/A:C).

Authentication Bypass

The device's web interface and the administrative web service do not consistently verify that web requests originate from authenticated sessions. Therefore it is possible for an attacker to bypass the login mechanism and modify device settings directly.

Applied Risk has calculated a CVSSv2 base score of 5.8 for this vulnerability; the CVSS vector string is (AV:A/AC:M/Au:N/C:C/I:C/A:C).

Persistent Cross Site Scripting

The device does not properly filter user input. Arbitrary JavaScript can be injected into any text parameter that is reflected in the device's web interface. Recent firmware versions provide a read-only interface, however malicious scripts can still be injected by other means, like e.g. through the GridVis management tool or directly through uploading FTP files.

Applied Risk has calculated a CVSSv2 base score of 5.5 for this vulnerability; the CVSS vector string is (AV:A/AC:M/Au:N/C:C/I:C/A:C).

Information disclosure

A service running on port 1234/UDP and port 1235/UDP expose netstat-like information, leaking info on current network sessions.

Applied Risk has calculated a CVSSv2 base score of 5 for this vulnerability; the CVSS vector string is (AV:A/AC:M/Au:N/C:C/I:C/A:C).

MITIGATION

Janitza has released updated firmware (r4061 build269) in order to address the reported issues; however it was observed that this update does not remediate all identified vulnerabilities.

The updated firmware causes the device to no longer expose the debug interface and connection information. In addition a lockout mechanism for the web interface login has been implemented, that locks the device for 10 minutes after 3 unsuccessful login attempts.

Furthermore Janitza has published a document which next to other security recommendations describes how to reconfigure the default password.

Besides upgrading to the latest firmware version it is recommended to shield the device from any publicly accessible networks by implementing proper network segregation and by filtering the exposed network services using a network firewall. Devices should be managed from a well secured management PC only, whilst not having any active web browser sessions with untrusted web sites.

REFERENCES

Vendor website

http://www.janitza.com

Product page

http://www.janitza.de/umg-605.html

Jasic programming language

http://www.janitza.de/jasic-merkmale.html

Manual “Secure TCP/IP Connection”

http://www.janitza.com/download-manuals-current-devices.html?file=files/download/manuals/Secure-TCPIP/20470140-Secure-connection.PDF

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-----
```