ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

ICS-CERT ADVISORY

ICSA-12-249-02—WAGO I/O SYSTEM 758 INSECURE CREDENTIAL VULNERABILITIES

September 05, 2012

OVERVIEW

This advisory updates the ICS-CERT Alert titled "ICS-ALERT-12-097-01—WAGO IPC Multiple Vulnerabilities" that was posted on the ICS-CERT Web site on April 06, 2012. This alert detailed a vulnerability report of "hard-coded" credentials and improper access controls in the WAGO I/O System 758 product line.

Researcher Reid Wightman of Digital Bond released these vulnerabilities without coordination with ICS-CERT or WAGO. After coordination with the researcher and the vendor, ICS-CERT determined that the improper authentication vulnerability is found in a third-party component used in multiple WAGO products. ICS-CERT is also coordinating this vulnerability with 3-S Smart Software Solutions, the third-party supplier. ICS-CERT will update an advisory with additional information from 3S as it becomes available.

WAGO has confirmed that its I/O System 758 products are configured with default operating system credentials. These credentials are disclosed, but WAGO provided no information on how to change the default passwords. WAGO has released a procedure with additional documentation on how to change the default operating system passwords in Models 758-874, 758-875, and 758-876. WAGO has also released a best security practices document that makes recommendations to its customers on how to best secure its industrial control system (ICS) products.

These vulnerabilities are exploitable remotely and proof-of-concept (PoC) exploits are known to exist.

AFFECTED PRODUCTS

The following WAGO products are affected:

- I/O System 758, Model 758-870,
- I/O System 758, Model 758-874,
- I/O System 758, Model 758-875, and

- I/O System 758, Model 758-876.

IMPACT

Attackers are able to exploit these vulnerabilities by using the default credentials to gain unauthorized administrative access to the systems.

Impact to individual organizations depends on many factors that are unique to each organization. ICS-CERT recommends that organizations evaluate the impact of these vulnerabilities based on their operational environment, architecture, and product implementation.

BACKGROUND

According to WAGO's Web site,[a] WAGO is an international company based in Germany. They operate production facilities in Germany, Switzerland, Poland, China, and India. WAGO maintains offices worldwide.

According to WAGO, its products are deployed across several sectors including manufacturing, building automation, electric generation, transportation, and others. WAGO estimates that these products are used worldwide.

VULNERABILITY CHARACTERIZATION

VULNERABILITY OVERVIEW

USE OF HARD-CODED PASSWORD[b]

The operating system software of the WAGO I/O System 758 product line uses three user accounts with default passwords and no method to change these passwords. An attacker could use the default password to gain administrative control through the Telnet service of the system leading to a loss of integrity, loss of confidentiality, or loss of availability.

a WAGO-USA, http://www.wago.us, Web site last accessed September 05, 2012.

b. CWE, http://cwe.mitre.org/data/definitions/259.html, CWE-259: Use of Hard-Coded Password, Web site last accessed September 05, 2012.

CVE-2012-3013[c] has been assigned to this vulnerability. A CVSS v2 base score of 10 has been assigned; the CVSS vector string is (AV:N/AC:L/Au:N/C:C/I:C/A:C).[d]

IMPROPER AUTHENTICATION[e]

WAGO IPCs offer the 3-S Smart Software Solutions CoDeSys runtime to program the IPC similar to a programmable logic controller. The CoDeSys software allows unauthenticated connections to the server to run arbitrary commands. This could allow possible remote code execution. A separate advisory with a CVE number and CVSS score will be published by ICS-CERT for this vulnerability as more information becomes available.

VULNERABILITY DETAILS

EXPLOITABILITY

These vulnerabilities could be remotely exploited.

EXISTENCE OF EXPLOIT

Public exploits are known to target these vulnerabilities.

DIFFICULTY

An attacker with a low skill level would be able to exploit these vulnerabilities.

MITIGATION

WAGO has developed a procedure[f] for the I/O System 758, Models 758-874, 758-875, and 758-876 that allows users to change passwords for their default operating system accounts. The WAGO Security Settings Application Note discusses changing the Web-based Management passwords as well as the Linux console passwords and list security recommendations for their customers. This procedure does not provide instructions to change the default passwords on the

c. NVD, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-3013, NIST uses this advisory to create the CVE Web site report. This Web site will be active sometime after publication of this advisory.
d. CVSS Calculator, http://nvd.nist.gov/cvss.cfm?version=2&vector=(AV:N/AC:L/Au:N/C:C/I:C/A:C), Web site last accessed September 05, 2012.
e. CWE, http://cwe.mitre.org/data/definitions/287.html, CWE-287: Improper Authentication, Web site last accessed September 05, 2012.
f. Security Settings in WAGO 758 Series IPCs, http://www.wago.com/wagoweb/documentation/app_note/a1176/a117600e.pdf, Web site last accessed September 05, 2012.

I/O System 758, Model 758-870 as it is no longer being produced. WAGO has released a cybersecurity notification[g] to its customers that details the best security settings and practices for its ICS products.

ICS-CERT encourages asset owners to take additional defensive measures to protect against this and other cybersecurity risks.

- Minimize network exposure for all control system devices. Critical devices should not directly face the Internet.
- Locate control system networks and remote devices behind firewalls, and isolate them from the business network.
- When remote access is required, use secure methods, such as Virtual Private Networks (VPNs), recognizing that VPN is only as secure as the connected devices.

The Control Systems Security Program (CSSP) also provides a section for control systems security recommended practices on the CSSP Web page. Several recommended practices are available for reading and download, including Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies.[h] ICS-CERT reminds organizations to perform proper impact analysis and risk assessment prior to taking defensive measures.

Organizations observing any suspected malicious activity should follow their established internal procedures and report their findings to ICS-CERT for tracking and correlation against other incidents.

ICS-CERT CONTACT

For any questions related to this report, please contact ICS-CERT at:

Email: ics-cert@dhs.gov
Toll Free: 1-877-776-7585
For CSSP Information and Incident Reporting: www.ics-cert.org

ICS-CERT continuously strives to improve its products and services. You can help by answering a short series of questions about this product at the following URL: https://forms.us-cert.gov/ncsd-feedback/.

g. WAGO Cybersecurity Notification, http://www.wago.us/products/40576.htm, Web site last accessed September 05, 2012.

h. CSSP Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html, Web site last accessed September 05, 2012.

DOCUMENT FAQ

What is an ICS-CERT Advisory? An ICS-CERT Advisory is intended to provide awareness or solicit feedback from critical infrastructure owners and operators concerning ongoing cyber events or activity with the potential to impact critical infrastructure computing networks.

When is vulnerability attribution provided to researchers? Attribution for vulnerability discovery is always provided to the vulnerability reporter unless the reporter notifies ICS-CERT that they wish to remain anonymous. ICS-CERT encourages researchers to coordinate vulnerability details before public release. The public release of vulnerability details prior to the development of proper mitigations may put industrial control systems and the public at avoidable risk.