ICS-CERT ALERT

ICS-ALERT-12-097-01—WAGO IPC MULTIPLE VULNERABILITIES

April 06, 2012

ALERT

SUMMARY

ICS-CERT is aware of a public report of multiple vulnerabilities affecting the WAGO IPC 758-870, which is an embedded Linux programmable logic controller (PLC). According to this report, an attacker could exploit these vulnerabilities to gain unauthorized access or to make unauthenticated configuration changes, which may include arbitrary code. The "Improper Access Control" vulnerability is the same vulnerability identified in ICS-ALERT-12-097-02—3S Software CoDeSys Improper Access Control.[a] This report was released by Reid Wightman, Digital Bond, without coordination with either the vendor or ICS-CERT.

ICS-CERT has notified the affected vendor of the report and has asked the vendor to confirm the vulnerability and identify mitigations. ICS-CERT is issuing this alert to provide early notice of the report and identify baseline mitigations for reducing risks to these and other cybersecurity attacks.

The report included vulnerability details for the following vulnerabilities:

Vulnerability Type	Exploitability	Impact
Use of Hard-coded Password	Remote	Loss of integrity
Improper Access Control	Remote	Loss of integrity, possible arbitrary code execution

Please report any issues affecting control systems in critical infrastructure environments to ICS-CERT.

MITIGATION

ICS-CERT is currently coordinating with the vendor and security researcher to identify mitigations.

ICS-CERT recommends that users take defensive measures to minimize the risk of exploitation of these vulnerabilities. Specifically, users should:

a. ICS-CERT ALERT, http://www.us-cert.gov/control_systems/pdf/ICS-ALERT-12-097-02.pdf, website last accessed April 5, 2012.

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

ICS-CERT reminds organizations to perform proper impact analysis and risk assessment prior to taking defensive measures.

The Control Systems Security Program (CSSP) also provides a recommended practices section for control systems on the US-CERT website. Several recommended practices are available for reading or download, including *Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies.*[c]

Organizations that observe 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

ICS-CERT Operations Center
1-877-776-7585
ics-cert@dhs.gov

For CSSP Information and Incident Reporting: www.ics-cert.org

DOCUMENT FAQ

What is an ICS-CERT Alert? An ICS-CERT Alert is intended to provide timely notification to critical infrastructure owners and operators concerning threats 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.

b. ICS-CERT ALERT, http://www.us-cert.gov/control_systems/pdf/ICS-Alert-10-301-01.pdf, website last accessed April 5, 2012.

c. Control System Security Program (CSSP) Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html, website last accessed April 5, 2012.