# ICS-CERT ALERT

## ICS-ALERT-12-020-07A—WAGO I/O 750 MULTIPLE VULNERABILITIES

**UPDATE A**

June 19, 2012

## ALERT

### SUMMARY

This Alert Update is a follow-up to the original ICS-CERT Alert titled ICS-ALERT-12-020-07—WAGO I/O 750 Multiple Vulnerabilities that was published January 20, 2012, on the ICS-CERT Web page.

**--------- Begin Update A Part 1 of 2 --------**

The reported vulnerabilities from DSecRG have been coordinated with WAGO. WAGO has determined that the vulnerabilities can be mitigated by adjusting system configurations of services not in use.

WAGO has released a customer cybersecurity notification on best security practices[a] for its products.

**--------- End Update A Part 1 of 2----------**

- ICS-CERT is aware of a public report of multiple vulnerabilities with proof-of-concept (PoC) exploit code affecting the WAGO I/O System 750, a controller product. According to the WAGO Web site, the WAGO I/O System 750 is used in the industrial automation, building automation, marine automation, and on and offshore applications. These reports were released by Digital Security Research Group (DSecRG) without coordination with either the vendor or ICS-CERT.
- ICS-CERT has notified WAGO of this 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.

a. WAGO Cybersecurity Notification, http://www.wago.us/products/40576.htm, Web site last accessed on July 19, 2012.

- The report included vulnerability details and PoC exploit code for the following vulnerabilities:

| Vulnerability Type | Exploitability | Impact |
|---|---|---|
| Data leakage | Remote | Download firmware |
| Data leakage | Remote | Data leakage |
| Unauthorized access | Remote | Denial of service/loss of system integrity |

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

## MITIGATION

ICS-CERT has coordinated with WAGO and the security researcher to identify mitigations. WAGO has determined that the reported vulnerabilities can be mitigated through system configuration.

**--------- Begin Update A Part 2 of 2 --------**

### DATA LEAKAGE RESULTING IN A DOWNLOAD OF FIRMWARE

In Section 10.4 of the WAGO I/O 750-841 User's Manual, Ports 44818/TCP and 2222/UDP can be disabled, thereby disabling the Web Based Management system preventing the download of firmware. WAGO recommends that these ports remain disabled when not being actively used. Section 12.1.1.5 recommends installing controllers behind firewalls.

### DATA LEAKAGE RESULTING IN LOSS OF CONFIDENTIALITY

In Section 10.4 of the WAGO I/O 750-841 User's Manual, Port 80/TCP can be disabled, thereby disabling the Web Based Management system. WAGO recommends that these ports remain disabled when not being actively used. Section 12.1.1.5 recommends using controllers behind firewalls.

### UNAUTHORIZED ACCESS RESULTING IN A DENIAL OF SERVICE OR LOSS OF SYSTEM INTEGRITY

The 750-841 provides a Web Server Authentication function. By default, this function is enabled, but it may be disabled. If enabled, the previous password must first be entered before the password can be changed. If disabled, the password may be changed without first entering

the previous password. WAGO recommends this function remain enabled. A description of the Web Server Authentication can be found in Section 10.8 of the WAGO I/O 750-841 User's Manual.

These features can be found in the WAGO I/O 750-841 User's Manual.[b]

**--------- End Update A Part 2 of 2----------**

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

- Minimize network exposure for all control system devices. Control system devices should not directly face the Internet.[c]
- 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 Web site. Several recommended practices are available for reading or download, including Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies.[d]

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
Email: ics-cert@dhs.gov

b. WAGO I/O 750-841User's Manual, http://www.wago.com/wagoweb/documentation/750/eng_manu/coupler_controller/m07500841_00000000_0en.pdf, Web site last accessed June 19, 2012.

c. ICS-CERT ALERT, http://www.us-cert.gov/control_systems/pdf/ICS-Alert-10-301-01.pdf, Web site last accessed June 19, 2012.

d. Control System Security Program (CSSP) Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html, Web site last accessed June 19, 2012.

## 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.