ICS-CERT ADVISORY

ICSA-12-249-01—ARBITER SYSTEMS POWER SENTINEL DENIAL-OF-SERVICE VULNERABILITY

September 05, 2012

OVERVIEW

Arbiter Systems reported to ICS-CERT that a vulnerability that causes a denial of service (DoS) has been identified in Arbiter Systems Power Sentinel Phasor Measurement Unit. The vulnerability can be exploited remotely. Arbiter Systems has produced a patch that mitigates this vulnerability. OSIsoft tested the patch to validate that it resolves the vulnerability.

AFFECTED PRODUCTS

The following Arbiter Systems Power Sentinel products are affected:

- Model 1133A Power Sentinel, firmware versions 09Jun2012 and earlier.

IMPACT

Successful exploitation of this vulnerability could lead to a DoS.

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

BACKGROUND

Arbiter Systems manufactures time clocks, power measurement, and power calibration products for use in electricity generation and transmission. These products are used primarily in the United States. Some are deployed to South America and Europe as well.

VULNERABILITY CHARACTERIZATION

VULNERABILITY OVERVIEW

DENIAL OF SERVICE[a]

The Ethernet port on this device stops responding to queries when its buffer is full. Certain types of queries to the Ethernet port, such as port scanning, cause the device to stop responding.

CVE-2012-3012[b] has been assigned to these vulnerabilities. A CVSS v2 base score of 7.8 has been assigned; the CVSS vector string is (AV:N/AC:L/Au:N/C:N/I:N/A:C).[c]

VULNERABILITY DETAILS

EXPLOITABILITY

This vulnerability can be exploited remotely.

EXISTENCE OF EXPLOIT

No known public exploits specifically target this vulnerability.

DIFFICULTY

An attacker with a low skill would be able to exploit this vulnerability.

MITIGATION

Arbiter Systems recommends that users update firmware to 11June2012 Rev 421 or later. This version is available on the product page for Model 1133A at the company Web site (http://www.arbiter.com/news/index.php?id=261). Users will need to download both the firmware as well as the uploader software to send the firmware to the device.

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

---

a. CWE-410: Insufficient Resource Pool, http://cwe.mitre.org/data/definitions/410.html, Web site last accessed September 05, 2012.

b. NVD, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-XXXX, NIST uses this advisory to create the CVE Web site report. This Web site will be active sometime after publication of this advisory.

c. CVSS Calculator, http://nvd.nist.gov/cvss.cfm?version=2&vector=(AV:N/AC:M/Au:N/C:N/I:N/A:C), Web site last accessed September 05, 2012.

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

Additional mitigation guidance and recommended practices are publicly available in the ICS-CERT Technical Information Paper ICS-TIP-12-146-01A—Cyber Intrusion Mitigation Strategies[e] that is available for download from the ICS-CERT Web page (www.ics-cert.org).

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/.

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

e. Cyber Intrusion Mitigation Strategies, http://www.us-cert.gov/control_systems/pdf/ICS-TIP-12-146-01A.pdf, 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.