ICS-CERT ADVISORY

ICSA-12-016-01—COGENT DATAHUB CROSS-SITE SCRIPTING AND HTTP HEADER INJECTION VULNERABILITIES

January 16, 2012

OVERVIEW

ICS-CERT is aware of a public report of multiple vulnerabilities in Cogent's DataHub application. These vulnerabilities include cross-site scripting and an HTTP header injection vulnerability, also known as a carriage return line feed. According to the report, Cogent Real-Times Systems Inc. has produced a patch that resolves these vulnerabilities.

Kuang-Chun Hung of Security Research and Service Institute - Information and Communication Security Technology Center (ICST), Taiwan R.O.C. reported these vulnerabilities to JPCERT/CC.

AFFECTED PRODUCTS

According to the report, the following products are affected:

- Cogent DataHub Version 7.1.2 and earlier
- OPC DataHub Version 6.4.20 and earlier
- Cascade DataHub Version 6.4.20 and earlier.

IMPACT

Successful exploitation of these vulnerabilities could result in one or more of the following:

- An arbitrary script being executed on the user's web browser
- Forged information may be displayed on the user's web browser
- An HTTP response splitting attack may be conducted.

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

Cogent Real-Time Systems Inc. is a Canadian-based company that produces middleware applications that are used to interface with control systems.

According to Cogent, DataHub is deployed across several sectors including manufacturing, building automation, chemical, banking and finance, electric utilities, and others. Cogent estimates these products are used primarily in the United States and Great Britain.

VULNERABILITY CHARACTERIZATION

VULNERABILITY OVERVIEW

CROSS-SITE SCRIPTING

A cross-site scripting vulnerability exists in the Cogent DataHub application because it lacks server-side validation of query string parameter values. Attacks that exploit these vulnerabilities require that a user visit a specially crafted URL, which injects client-side scripts into the server's HTTP response to the client.

CVE-2012-0309[a] has been assigned to this vulnerability. A CVSS V2 base score of 4.3 has also been assigned.

HTTP HEADER INJECTION VULNERABILITY

An HTTP header injection vulnerability (also known as carriage return line feed) exists in the Cogent DataHub application as the product does not validate or incorrectly validates input that can affect the control flow or data flow of a program.

CVE-2012-0310[b] has been assigned to this vulnerability. A CVSS V2 base score of 4.3 has also been assigned.

VULNERABILITY DETAILS

EXPLOITABILITY

This vulnerability is remotely exploitable but may social engineering.

a. http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-0309, website last accessed January 13, 2012
b. http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-0310, website last accessed January 13, 2012

EXISTENCE OF EXPLOIT

No known exploits specifically target this vulnerability.

DIFFICULTY

An attacker with a low to moderate skill level could exploit these vulnerabilities.

MITIGATION

According to the report, Cogent Real-Time Systems In. has produced a patch for these vulnerabilities that can be obtained by accessing the Cogent website located here: http://www.cogentdatahub.com/Contact_Form.html and filling out the required information.

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.*[c] 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.

In addition, ICS-CERT recommends that users take the following measures to protect themselves from social engineering attacks:

1. Do not click web links or open unsolicited attachments in e-mail messages

c. CSSP Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html, website last accessed January 13, 2012.

2. Refer to *Recognizing and Avoiding Email Scams* [d] for more information on avoiding e-mail scams
3. Refer to *Avoiding Social Engineering and Phishing Attacks* [e] for more information on social engineering attacks.

ICS-CERT CONTACT

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

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

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.

d. Recognizing and Avoiding Email Scams, http://www.us-cert.gov/reading_room/emailscams_0905.pdf, website last accessed January 13, 2012
e. National Cyber Alert System Cyber Security Tip ST04-014, http://www.us-cert.gov/cas/tips/ST04-014.html, website last accessed January 13, 2012