ICS-CERT ADVISORY

ICSA-11-280-01— COGENT DATAHUB MULTIPLE VULNERBILITIES

October 07, 2011

OVERVIEW

This Advisory is a follow-up to the Alert, "ICS-ALERT-11-256-03—COGENT DATAHUB MULTIPLE VULNERABILITIES," that was published September 13, 2011, on the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) web page.

ICS-CERT is aware of a public report of multiple vulnerabilities in Cogent's DataHub application. These vulnerabilities include denial-of-service, information leakage, and remote code execution. Cogent has produced a patch that resolves these vulnerabilities in DataHub.

AFFECTED PRODUCTS

According to Cogent, the following products are affected:

- Cogent DataHub all of Version 7 until 7.1.2
- OPC DataHub prior to Version 6.4.20
- Cascade DataHub all of Version 6 6.4.20.

IMPACT

Successful exploitation of this vulnerability could result in denial-of-service, data leakage, or remote code execution.

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 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

STACK UNICODE OVERFLOW

A Stack Unicode Overflow can occur when a specially crafted packet is sent to Port 4502\Transmission Control Protocol (TCP) or Port 4503\TCP. This attack only affects Cogent DataHub v7. Successful exploitation could lead to denial-of-service or remote code execution.

CVE-2011-3493 has been assigned to this vulnerability.[a] A CVSS v2 base score of 10.0 has also been assigned.

DIRECTORY TRAVERSAL

A directory traversal vulnerability can occur when a specially crafted request is passed to the web server running on Port 80\TCP. Successful exploitation could result in data leakage.

CVE-2011-3500 has been assigned to this vulnerability.[b] A CVSS v2 base score of 5.0 has also been assigned.

INTEGER OVERFLOW

An Integer Overflow can occur when a specially crafted packet is sent to Port 80\TCP. Successful exploitation could lead to denial-of-service.

CVE-2011-3501 has been assigned to this vulnerability.[c] A CVSS v2 base score of 5.0 has also been assigned.

SOURCE DISCLOSURE

A Source Disclosure vulnerability can occur when a specially crafted request is passed to the web server running on Port 80\TCP. Successful exploitation could result in data leakage.

CVE-2011-3502 has been assigned to this vulnerability.[d] A CVSS v2 base score of 5.0 has also been assigned.

a. http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-3493 , website last access October 04, 2011.
b. http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-3500 , website last access October 04, 2011.
c. http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-3501, website last access October 04, 2011.
d. http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-3502 , website last access October 04, 2011

VULNERABILITY DETAILS

EXPLOITABILITY

These vulnerabilities are remotely exploitable.

EXISTENCE OF EXPLOIT

Public exploit(s) are known to target these vulnerabilities.

DIFFICULTY

An attacker with a low skill level can create the denial-of-service and data leakage, whereas it would require a more skilled attacker to execute arbitrary code.

MITIGATION

Cogent recommends the following mitigation strategies.

- Turn off Ports 4502\TCP and 4503\TCP if they are not in use. This can be done in the Tunnel/Mirror properties of Datahub.
- If Ports 4502\TCP and 4503\TCP are in use, configure authentication on all TCP connections. Instructions for doing this are below.

    1. Remove all permissions for the special user names "TCP" and "Mirror" in the security properties of the DataHub.
    2. Create a group for users who are authorized, and allow "BasicConnectivity" for that group. The DataHub will then refuse all commands from unauthenticated TCP connections, and still allow authenticated users to connect.[e]

- If DataHub Web Server is not being used, turn it off in the Web Server properties.
- If DataHub Web Server is exposed to the Internet, configure user and password authentication.[f]
- In both cases, if access to DataHub from the Internet is not required, block Ports 4502\TCP, 4503\TCP, 80\TCP, and 943\TCP at your firewall, and only allow connections on these ports from within your local area network.
- Upgrade to Version 7.1.2 of DataHub or Version 6.4.20 of the OPC DataHub or Cascade DataHub if running in an untrusted environment.[g]

e. http://www.cogentdatahub.com/Docs/cdh-dhsecurity.html , website last access October 04, 2011.
f. http://www.cogentdatahub.com/Docs/cdh-webcreatingpasswords.html , website last access October 04, 2011.
g. http://www.cogentdatahub.com/Download.html, website last access October 04, 2011.

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 system 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:

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 provided when prior coordination has occurred with either the vendor, ICS-CERT, or other coordinating entity. 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 (ICSs) and the public at avoidable risk.

h. CSSP Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html, website last access, October 04, 2011.