ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

ICS-CERT ADVISORY

ICSA-13-095-01 COGENT REAL-TIME SYSTEMS MULTIPLE VULNERABILITIES

April 5, 2013

OVERVIEW

Dillon Beresford of Cimation has identified multiple vulnerabilities in the Cogent Real-Time Systems DataHub application. Cogent has produced an update that mitigates these vulnerabilities. These vulnerabilities could be exploited remotely.

AFFECTED PRODUCTS

Cogent Real-Time Systems reports that these vulnerabilities affect the following versions:

- Cogent DataHub Version 7.2.2 and earlier,
- OPC DataHub Version 6.4.21 and earlier,
- Cascade DataHub for Windows Version 6.4.21 and earlier,
- DataSim and DataPid demonstration clients for Cogent DataHub V7.2.2,
- DataSim and DataPid demonstration clients for OPC DataHub and Cascade DataHub V6.4.21, and
- DataHub QuickTrend Version 7.2.2 and earlier.

IMPACT

Successful exploitation of these vulnerabilities will cause the affected programs to terminate, causing a denial of service (DoS). Other exploitations of these vulnerabilities may also allow an

attacker to alter the program stack or allow the attacker to execute arbitrary code in the context of the applications.

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.

Cogent's products are deployed across several sectors including manufacturing, building automation, chemical, banking and finance, electric utilities, and others. These products are used worldwide, primarily in the United States and Great Britain.

VULNERABILITY CHARACTERIZATION

VULNERABILITY OVERVIEW

IMPROPER INPUT VALIDATION[a]

The DataHub application accepts formatted text commands via a TCP connection on Ports 4502/TCP and 4503/TCP. These commands are parsed, validated, and executed within the application. The parser contains an error where malformed input will cause the parser to perform a reference through a NULL pointer, causing the application to crash.

CVE-2013-0681[b] has been assigned to this vulnerability. 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]

a. CWE-20: Improper Input Validation, http://cwe.mitre.org/data/definitions/20.html, Web site last accessed April 04, 2013.

b. NVD, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2013-0681, 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:L/Au:N/C:N/I:N/A:C), Web site last visited April 04, 2013.

BUFFER OVERFLOW[d]

The DataHub application contains a built-in Web server that will accept HTTP requests via Port 80/TCP. An attacker could send an HTTP request with an unusually long header parameter, causing a stack buffer overflow within the Web server. Typically, this will lead to an application crash, causing a DoS. In theory, a carefully constructed header could be used to overwrite the stack in a predictable way, leading to arbitrary code execution.

CVE-2013-0680[e] has been assigned to this vulnerability. A CVSS v2 base score of 8.5 has been assigned; the CVSS vector string is (AV:N/AC:L/Au:N/C:N/I:P/A:C).[f]

INVALID POINTER[g]

The DataSim and DataPid programs connect to the DataHub via a TCP connection. Information and commands are exchanged via formatted text messages over this connection. If the user connects DataSim or DataPid to a server other than the DataHub, and this server is designed to generate random or malformed messages, then DataSim and DataPid could crash.

In order to exploit this scenario, an attacker would need to induce the user to connect DataSim and DataPid to a server other than the DataHub. The simple act of inducing this connection would mean that the data produced by DataPid and DataSim would not be connected to the production system and no data would be delivered to the DataHub. Subsequently, causing DataSim and DataPid to crash would produce no further negative effect on the system. Consequently, this crash scenario does not constitute a DoS.

DataSim and DataPid are not used in production systems and do not pose a risk.

CVE-2013-0683[h] has been assigned to this vulnerability. A CVSS v2 base score of 7.1 has been assigned; the CVSS vector string is (AV:N/AC:M/Au:N/C:N/I:N/A:C).[i]

d. CWE-20: Improper Input Validation, http://cwe.mitre.org/data/definitions/20.html, Web site last accessed April 04, 2013.

e. NVD, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2013-0680, NIST uses this advisory to create the CVE Web site report. This Web site will be active sometime after publication of this advisory.

f. CVSS Calculator, http://nvd.nist.gov/cvss.cfm?version=2&vector=(AV:N/AC:L/Au:N/C:N/I:P/A:C), Web site last visited April 04, 2013.

g. CWE-763: Release of Invalid Pointer or Reference, http://cwe.mitre.org/data/definitions/763.html, Web site last accessed April 04, 2013.

h. NVD, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2013-0683, NIST uses this advisory to create the CVE Web site report. This Web site will be active sometime after publication of this advisory.

ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

IMPROPER EXCEPTION HANDLING[j]

The DataHub application accepts formatted text commands via a TCP connection. These commands are parsed, validated, and executed within the application. When the parser is sent random data, it may access memory beyond the end of an allocated heap buffer, causing a crash. It may also access memory beyond the end of a stack buffer, providing an opportunity for a carefully crafted message to modify the stack to allow code execution.

CVE-2013-0682[k] has been assigned to this vulnerability. A CVSS v2 base score of 8.5 has been assigned; the CVSS vector string is (AV:N/AC:L/Au:N/C:N/I:P/A:C).[l]

VULNERABILITY DETAILS

EXPLOITABILITY

These vulnerabilities could be exploited remotely.

EXISTENCE OF EXPLOIT

No known public exploits specifically target these vulnerabilities.

DIFFICULTY

An attacker with a low skill would be able to exploit these vulnerabilities. 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 being used. This can be done in the Tunnel/Mirror properties of the DataHub.

i. 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 visited April 04, 2013.

j. CWE-755: Improper Handling of Exceptional Conditions, http://cwe.mitre.org/data/definitions/755.html , Web site last accessed April 04, 2013.

k. NVD, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2013-0682 , NIST uses this advisory to create the CVE Web site report. This Web site will be active sometime after publication of this advisory.

l. CVSS Calculator, http://nvd.nist.gov/cvss.cfm?version=2&vector=(AV:N/AC:L/Au:N/C:N/I:P/A:C), Web site last visited April 04, 2013.

- If access to the application from the Internet is not required, block Ports 4502/TCP and 4503/TCP at your firewall, and only allow connections on these ports from within your local area network.
- If the DataHub Web server is not being used, turn it off in the Web server properties.
- If access to DataHub from the Internet is not required, block Port 80/TCP at your firewall, and only allow connections on this port from within your local area network.
- This vulnerability is fixed in the following software versions. Upgrade to one of these applications.
  - DataHub QuickTrend Version 7.3.0
  - Cogent DataHub Version 7.3.0
  - OPC DataHub Version 6.4.22
  - Cascade DataHub for Windows Version 6.4.22.

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.

ICS-CERT also provides a section for control systems security recommended practices on the ICS-CERT Web page. Several recommended practices are available for reading and download, including Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies.[m] 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-12-146-01B—Targeted Cyber Intrusion

m. CSSP Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html, Web site last accessed April 04, 2013.

Detection and Mitigation Strategies,[n] 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@hq.dhs.gov
Toll Free: 1-877-776-7585
For industrial control systems security 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/.

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.

I see that this document is labeled as TLP = WHITE. May I distribute this to other people? According to the International Critical Information Infrastructure Protection (CIIP) Traffic Light Protocol[o,p] warning, this document is subject to standard copyright rule and may be distributed freely without restriction.
TLP = WHITE: Unlimited

n. Cyber Intrusion Mitigation Strategies, http://www.us-cert.gov/control_systems/pdf/ICS-TIP-12-146-01B.pdf, Web site last accessed April 04, 2013.

o. Traffic Light Protocol—International CIIP Directory, Issue 21, March 29, 2013.

p. US-CERT, http://www.us-cert.gov/tlp/, Web site last accessed April 04, 2013.