



ICS-CERT

INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

ICS-CERT ALERT

ICS-ALERT-11-256-03—COGENT DATAHUB MULTIPLE VULNERABILITIES

September 13, 2011

ALERT

SUMMARY

ICS-CERT is aware of a public report of four vulnerabilities with proof of concept (POC) exploit code affecting Cogent DataHub. According to the reports, the vulnerabilities are remotely exploitable through ports that are listed in the table below. This report was released without coordination with the vendor or with ICS-CERT.

ICS-CERT has not yet verified the vulnerabilities or POC code, but has reached out to the affected vendor to notify, confirm, 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.

The report included vulnerability details and proof-of-concept exploit code for the following vulnerabilities:

Vulnerability Type	Exploitability	Impact
Stack Overflow	Remote – Ports 4052 and 4053	Denial of Service / Possible Remote Code Execution
Integer Overflow	Remote – Port 80	Denial of Service
Directory Traversal	Remote – Port 80	Information Leak / Disclosure
Information Exposure	Remote – Port 80	Information Leak / Disclosure

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

BACKGROUND

Cogent DataHub is SCADA management software used in many industries including manufacturing, energy, financial, and pharmaceuticals.

MITIGATION

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



ICS-CERT

INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

- Minimize network exposure for all control system devices. Control system devices should not directly face the Internet.^a
- 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).

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

The Control System Security Program also provides a recommended practices section for control systems on the US-CERT website. Several recommended practices are available for reading or download, including *Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies*.^b

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

ICS-CERT@DHS.GOV

For Control Systems Security Program (CSSP) Information and Incident Reporting: www.ics-cert.org

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.

a. ICS-CERT ALERT, http://www.us-cert.gov/control_systems/pdf/ICS-Alert-10-301-01.pdf, accessed September 13, 2011.

b. Control System Security Program (CSSP) Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html, accessed September 13, 2011.