ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

ICS-CERT ADVISORY

ICSA-11-264-01—AZEOTECH DAQFACTORY STACK OVERFLOW

September 21, 2011

OVERVIEW

This advisory is a follow-up to the alert titled “ICS-ALERT-11-256-02—AzeoTech DAQFactory Stack Overflow” that was published September 13, 2011, on the ICS-CERT web page.

ICS-CERT is aware of a public report of one stack overflow vulnerability with proof-of-concept (POC) exploit code affecting AzeoTech DAQFactory, a SCADA/HMI Product. According to the report, the vulnerability is exploitable via a service running on Port 20034/UDP. The report was released without coordinating with either the vendor or ICS-CERT. ICS-CERT has coordinated with AzeoTech, which has produced an upgrade that resolves the vulnerability. ICS-CERT has not validated the upgrade.

Attribution for the vulnerability discovery is not provided in this advisory because no prior coordination occurred with the vendor, ICS-CERT, or other coordinating body. 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.

AFFECTED PRODUCTS

According to AzeoTech, only DAQFactory Version 5.85 is affected by this vulnerability.

IMPACT

This stack overflow vulnerability could allow an attacker to cause a denial of service or remotely execute code on the targeted system.

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

BACKGROUND

DAQFactory is a supervisory control and data acquisition (SCADA) and human-machine interface (HMI) software used in multiple industries including water, power, and manufacturing. DAQFactory installations are primarily located in the United States and Europe.

VULNERABILITY CHARACTERIZATION

VULNERABILITY OVERVIEW

DAQFactory listens on Port 20034/UDP by default. An attacker can send specially crafted traffic to this port to cause a stack overflow, which may allow remote code execution.

MITRE[a] has assigned number CVE-2011-3492 to this vulnerability in the Common Vulnerabilities and Exposures (CVE) database.

VULNERABILITY DETAILS

EXPLOITABILITY

This vulnerability is remotely exploitable.

EXISTENCE OF EXPLOIT

Public exploits are known to target this vulnerability.

DIFFICULTY

An attacker with a low skill level can create the denial of service; however, only a more skilled attacker could exploit this vulnerability to execute arbitrary code.

MITIGATION

According to AzeoTech, the vulnerable feature has been completely removed in the next version (Version 5.86). The feature was undocumented, and AzeoTech does not believe it was being used by any of their customers. Therefore, its removal should not adversely affect any DAQFactory users.

AzeoTech provides the following instructions to upgrade to Version 5.86:

Existing customers can download and install the DAQFactory trial from the website (http://www.AzeoTech.com/downloads.php) over their existing installation at no charge. The user's license is maintained. Because this is the standard update path for DAQFactory, most customers will be familiar with the process.

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

[a] http://cve.mitre.org/cve, website last accessed September 21 2011.

- 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.*[b] 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.

[b] CSSP Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html, website last accessed September 21, 2011.