ICS-CERT ADVISORY

ICSA-11-122-01—AZEOTECH DAQFACTORY NETWORKING VULNERABILITIES

June 24, 2011

OVERVIEW

ICS-CERT Advisory ICSA-11-122-01 was originally released to the US-CERT Portal on May 24, 2011. This web page release was delayed to allow users sufficient time to download and install the upgrade.

ICS-CERT received a report from the nSense Vulnerability Coordination Team concerning several vulnerabilities in AzeoTech DAQFactory. ICS-CERT has worked with nSense and AzeoTech to validate the vulnerabilities and create a mitigation strategy, included below. Azeotech has created a new version (Version 5.85, Build 1842) to resolve these vulnerabilities. Users who do not require the networking capability can easily adjust the system settings in their existing versions to disable the vulnerable feature. The default settings for future releases (Versions 5.85 and newer) will be changed to mitigate the vulnerability. ICS-CERT has confirmed that both Version 5.85 and disabling the vulnerable feature in older versions successfully mitigates this vulnerability.

AFFECTED PRODUCTS

AzeoTech reports that the DAQFactory networking vulnerability only affects users of DAQFactory Standard, Pro, Developer, or Runtime. DAQFactory Express, Starter, Lite, and Base do not support networking and are not vulnerable to these attacks.

IMPACT

When the affected networking features of DAQFactory are enabled and the system is in an insecure position (e.g., facing the Internet without a properly configured firewall and/or relying on default passwords), an attacker can cause the system to stop functioning or reboot.

BACKGROUND

AzeoTech provides supervisory control and data acquisition (SCADA) and human-machine interface software to customers in multiple industries, including water, power, and manufacturing. AzeoTech customers are located primarily in the United States and Europe, but are also in other parts of the world.

VULNERABILITY CHARACTERIZATION

VULNERABILITY OVERVIEW

The DAQFactory networking feature allows multiple machines running DAQFactory to interact with each other. This interaction includes sending a signal from one device to initiate a reboot or shut down of another device. Because these signals are not encrypted or otherwise protected, a successful attacker could trigger a DAQFactory system reboot or shutdown.

VULNERABILITY DETAILS

EXPLOITABILITY

This vulnerability is remotely exploitable.

EXISTENCE OF EXPLOIT

No exploits are known that specifically target this vulnerability.

DIFFICULTY

An attacker would require basic skills to exploit this vulnerability.

MITIGATION

AzeoTech recommends that users take one of the following steps to secure their systems:

1. Upgrade to Version 5.85 (Build 1842), which addresses this vulnerability by adding authentication, and changes default settings to disable both the networking feature and also the remote reboot and shutdown feature. Users can download Version 5.85 at: www.azeotech.com/downloads.php.
2. For versions older than Version 5.85, disable the DAQFactory networking feature if the system configuration does not require network support. Users can check the “Disable Broadcast” option in the “File - Document Settings” menu.
3. AzeoTech recommends that DAQFactory only be deployed on an isolated network when one of the above mitigation steps cannot be performed.

ICS-CERT has verified that upgrading to Version 5.85 (Build 1842) successfully mitigates the reported vulnerabilities.

ICS-CERT encourages asset owners to 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 business networks. When remote access is required, use secure methods such as Virtual Private Networks (VPNs).

Organizations observing 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 reminds organizations to perform proper impact analysis and risk assessment prior to taking defensive measures.

The Control Systems Security Program (CSSP) also provides a recommended practices section for control systems on the CSSP web page. Several recommended practices are available for reading or download, including *Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies.*[a]

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.

[a] CSSP Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html, website last accessed May 20, 2011.