ICS-CERT ADVISORY

ICSA-11-279-04— BECKHOFF TWINCAT DENIAL-OF-SERVICE VULNERABILITY

October 06, 2011

OVERVIEW

This Advisory is a follow-up to the Alert, "ICS-ALERT-11-256-06— BECKHOFF TWINCAT DENIAL OF SERVICE VULNERABILITY,"[a] 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 a denial-of-service vulnerability as a result of a read access violation in Beckhoff's TwinCAT Software. Beckhoff has produced a patch to address this vulnerability in TwinCAT Software.

AFFECTED PRODUCTS

According to Beckhoff, the following product is affected:

- TwinCAT versions 2.10, 2.11, 2.11R2

IMPACT

Successful exploitation of this vulnerability could result in a denial-of-service.

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

Beckhoff is a German-based company that provides industrial automation control and information products worldwide, across a wide range of industries.

According to Beckhoff, TwinCAT is deployed across several sectors including general and special purpose machine building, manufacturing, building automation, oil and gas, water and wastewater, electric utilities, renewable energies, and others and is deployed worldwide.

[a] http://www.us-cert.gov/control_systems/pdf/ICS-ALERT-11-256-06.pdf, website last accessed October 06, 2011

VULNERABILITY CHARACTERIZATION

VULNERABILITY OVERVIEW

A read access violation can occur when a specially crafted packet is sent to Port 48899\UDP.

CVE-2011-3486 has been assigned to this vulnerability[b]. A CVSS base score of 5.0 has also been assigned.

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.

MITIGATION

Beckhoff has developed a patch to address this vulnerability. To obtain the patch and installation instructions, customers should contact Beckhoff at patch@beckhoff.com.

If the customer is unable to apply the patch, Beckhoff recommends that customers deploy a firewall and restrict traffic on the affected port (48899\UDP).

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.

[b] http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-3486, website last accessed October 06, 2011.

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 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.*[c]

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.

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