ICS-CERT

INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

ICS-CERT ADVISORY

ICSA-11-216-01—SCADATEC PROCYON TELNET BUFFER OVERFLOW VULNERABILITY

September 06, 2011

OVERVIEW

ICS-CERT originally released Advisory ICSA-11-216-01P on the US-CERT Portal on August 04, 2011. This web page release was delayed to allow users sufficient time to download and install the update.

ICS-CERT has received a report from Knud Højgaard of the nSense Vulnerability Coordination Team concerning a vulnerability in the Scadatec Limited Procyon human-machine interface/supervisory control and data acquisition (HMI/SCADA) product. This vulnerability could allow an attacker to establish a connection to the Telnet daemon, bypassing proper authentication, and exploit a buffer overflow that could lead to a denial of service (DoS) or remote code execution.

ICS-CERT has been working with nSense and Scadatec Limited to validate this vulnerability. Scadatec Limited has created a new version (V1.14) of the Procyon product that fully resolves this issue. nSense has confirmed that Procyon Version V1.14 successfully resolves this vulnerability.

AFFECTED PRODUCTS

Scadatec Procyon HMI prior to Version 1.14.

IMPACT

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 operational environment, architecture, and product implementation.

BACKGROUND

Procyon is an HMI product used in a variety of industrial applications that is produced by Scadatec Limited. According to Scadatec Limited, Procyon has known deployments in the UK, Philippines, Thailand, and Singapore. The total deployment of Procyon is not known because of distribution through third-party agents worldwide.

Procyon is more widely distributed in manufacturing and transportation applications with a lesser presence in the laboratory, water, and chemical applications.

VULNERABILITY CHARACTERIZATION

VULNERABILITY OVERVIEW

According to the researcher's report, the Scadatec Procyon Telnet service listening on Port 23/TCP is vulnerable to a buffer overflow[a] that could allow a DoS or possibly lead to arbitrary code execution. This vulnerability is remotely exploitable.

MITRE[b] has assigned number CVE-2011-3322 to this vulnerability.

VULNERABILITY DETAILS

EXPLOITABILITY

This vulnerability is remotely exploitable. In order to exploit this vulnerability, an attacker would need to send a specially crafted packet to Port 23/TCP that could cause a buffer overflow, resulting in an arbitrary code execution.

EXISTENCE OF EXPLOIT

No known exploits specifically target this vulnerability.

DIFFICULTY

Creating a working exploit for this vulnerability requires a low to moderate skillset.

MITIGATION

Scadatec Limited has produced a new version of the affected software available at the website listed below. Scadatec Limited has requested customers needing this new version to access this website, use the "Contact" tab to reach the "Contact Us" window, fill out and submit the form. This will alert Scadatec Limited to send the requester the required password to download this new version: http://scadatec.co.uk/existing_users.html

After downloading the new version, Scadatec Limited recommends the following actions:

- First, review the instructions in the Readme file.
- Uninstall any existing version of the software.
- Install the new version and run as normal.

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

[a] http://cwe.mitre.org/data/definitions/121.html, website last accessed September 02, 2011.

[b] http://cve.mitre.org/cve/, website last accessed September 06, 2011.

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.

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

The Control Systems Security Program (CSSP) 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]

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.

[c] CSSP Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html, website last accessed September 06, 2011.