ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

ICS-CERT ADVISORY

ICSA-11-277-01—SCHNEIDER ELECTRIC UNITELWAY DEVICE DRIVER BUFFER OVERFLOW

October 20, 2011

OVERVIEW

ICS-CERT originally released Advisory ICSA-11-277-01P on the US-CERT secure Portal on October 04, 2011. This web page release was delayed to allow users sufficient time to download and install the update.

Researcher Kuang-Chun Hung of Security Research and Service Institute - Information and Communication Security Technology Center (ICST) has identified a buffer overflow vulnerability in UnitelWay Windows Device Driver. This device driver is deployed as part of several different Schneider Electric products.

ICS-CERT has coordinated this vulnerability report with Schneider Electric. The vendor has produced a fix that resolves this vulnerability. ICST has successfully tested and validated that this fix fully resolves this vulnerability.

AFFECTED PRODUCTS

The following software packages are affected:

Product	Version	Platform
Unity Pro	Version 6 and prior	Windows XP
OPC Factory Server	Version 3.34	Windows XP
Vijeo Citect	Version 7.20 and prior	Windows XP
Telemecanique Driver Pack	Version 2.6 and prior	Windows XP
Monitor Pro	Version 7.6 and prior	Windows XP
PL7 Pro	Version 4.5 and prior	Windows XP

These six products are known to have the vulnerable UnitelWay Windows Device Driver and are elements of Schneider Electric SoCollaborative software components. These components are part of Schneider Electric process automation architecture known as PlantStruxure.

IMPACT

Exploitation of this vulnerability will allow an attacker to run arbitrary 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

Schneider Electric is a manufacturer and integrator of energy management equipment and software. Schneider Electric systems are found in the energy, manufacturing, building automation, and information technology. Schneider Electric reports operations in over 100 countries worldwide.

VULNERABILITY CHARACTERIZATION

VULNERABILITY OVERVIEW

An oversized input string to a parameter in this system using the UnitelWay Windows Device Driver causes a buffer overflow that allows arbitrary code execution.

CVE-2011-3330[a] has been assigned to this vulnerability.

VULNERABILITY DETAILS

EXPLOITABILITY

This vulnerability is not remotely exploitable.

EXISTENCE OF EXPLOIT

No known exploits specifically target this vulnerability.

DIFFICULTY

An attacker with a low skill level can create a denial of service whereas it would require a more skilled attacker to execute arbitrary code.

MITIGATION

Schneider Electric has created a fix that modifies one of the libraries of the UnitelWay Windows Device Driver. Schneider Electric has also issued a customer notification describing the vulnerability.[b] Schneider

[a] http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-3330 , website last accessed October 20, 2011

[b] Vulnerability within UnitelWay Windows Device Driver, http://www.scada.schneider-electric.com/sites/scada/en/login/vijeo-citect-unitelway-windows-device-driver.page, website last accessed October 20, 2011.

Electric recommends that since the functionality of the existing version is not affected by the installation of the fix, all customers should install the fix, which is available at the following address:

www.scada.schneider-electric.com/download/security/HFPEP0047398R.zip

Schneider Electric recommends that customers requiring additional assistance contact their global support center or a local customer service center. Contact information is available at the following web addresses.

Vijeo Citect customers should contact Schneider Electric's SCADA and MES Software Support Center: http://www.scada.schneider-electric.com/sites/scada/en/login/country-support.page

Customers of all other affected Schneider Electric products should contact their local support center: http://www2.schneider-electric.com/sites/corporate/en/support/operations/local-operations/local-operations.page

In addition to applying the fix developed by Schneider Electric, ICS-CERT encourages asset owners to take additional defensive measures against this and other cybersecurity threats by:

- Minimizing network exposure for all control system devices. Critical devices should not directly face the Internet.
- Locating control system networks and remote devices behind firewalls, and isolate them from the business network.
- When remote access is required, using secure methods, such as Virtual Private Networks (VPNs), recognizing that VPN is only as secure as the connected devices.

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.*[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

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

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.