ICS-CERT

INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

ICS-CERT ADVISORY

ICSA-11-279-03—UNITRONICS UNIOPC SERVER INPUT HANDLING VULNERABILITY

October 06, 2011

OVERVIEW

Independent security researchers Billy Rios and Terry McCorkle have identified a vulnerability in Unitronics' UniOPC Server product. This vulnerability is a result of improper handling of input by a third-party component, https.ocx, which is part of "IP*Works! SSL". IP*Works! is used in the UniOPC product. Successful exploitation of this vulnerability results in a crash and could result in the execution of arbitrary code.

Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) has coordinated with Unitronics and the security researchers. Unitronics has released a new version that does not contain the vulnerable component. The researchers have confirmed that the vulnerable component is not present in the new version. However, customers installing the new version on a system that had previously contained an affected version of UniOPC are still vulnerable as the update does not remove the vulnerable component.

AFFECTED PRODUCTS

This vulnerability affects versions of Unitronics UniOPC prior to Version 2.0.0.

IMPACT

Exploitation of this vulnerability could result in the execution of arbitrary code on a system running an affected version of the Unitronics UniOPC product.

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

Unitronics is based in Israel. UniOPC Server provides the ability to read and write data between Unitronics programmable logic controllers (PLCs) and other applications that support OLE for Personal Computers (OPC). UniOPC Server is a standalone product that runs independently of other Unitronics software.

According to Unitronics, UniOPC is used worldwide in multiple sectors.

VULNERABILITY CHARACTERIZATION

VULNERABILITY OVERVIEW

This vulnerability resides in the https.ocx component of “IP*Works! SSL”[a] that is used as part of the Unitronics UniOPC product. An attacker could build a specially crafted website that accesses the vulnerable function to cause a crash and potentially execute arbitrary code.

VULNERABILITY DETAILS

EXPLOITABILITY

This vulnerability is remotely exploitable.

EXISTENCE OF EXPLOIT

No known exploits specifically target this vulnerability.

DIFFICULTY

An attacker with a low to medium skill level may exploit this vulnerability.

MITIGATION

Unitronics has released Version 2.0.0 of UniOPC Server. Unitronics recommends that users of all versions of the UniOPC Server product download and install Version 2.0.0 or newer from the following location:

http://www.unitronics.com/Content.aspx?page=Downloads

Unitronics has not provided mitigation steps for existing customers who are currently using affected versions of UniOPC. The vulnerable component will remain on the system even after the new version has been installed.

To manually remove the vulnerable component, the researcher suggests the following steps:

1. Ensure that no other applications are using https50.ocx prior to its removal.
2. From a command prompt type: regsvr32 /U c:\windows\system32\https50.ocx
3. Delete the c:\windows\system32\https50.ocx file.

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

[a] /n Software: IP*Works! SSL, http://www.nsoftware.com/ipworks/ssl/, website last accessed October 06, 2011.

In addition to installing the latest version of UniOPC Server, ICS-CERT encourages asset owners to take additional defensive measures to protect their systems from this and other vulnerabilities.

- 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]

In addition, ICS-CERT recommends that users take the following measures to protect themselves from social engineering attacks:

1. Do not click web links or open unsolicited attachments in e-mail messages
2. Refer to *Recognizing and Avoiding Email Scams*[c] for more information on avoiding e-mail scams
3. Refer to *Avoiding Social Engineering and Phishing Attacks*[d] for more information on social engineering attacks.

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

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

[c] Recognizing and Avoiding Email Scams, http://www.us-cert.gov/reading_room/emailscams_0905.pdf, website last accessed October 06, 2011.

[d] National Cyber Alert System Cyber Security Tip ST04-014, http://www.us-cert.gov/cas/tips/ST04-014.html, website last accessed October 06, 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.