ICS-CERT ADVISORY

ICSA-12-013-01—ING. PUNZENBERGER COPA-DATA GMBH DENIAL-OF-SERVICE VULNERABILITIES

February 07, 2012

OVERVIEW

ICS-CERT originally released Advisory ICSA-12-013-01P on the US-CERT secure portal on January 13, 2012. This web page release was delayed to allow users time to download and install the update.

Researcher Kuang-Chun Hung of the Security Research and Service Institute—Information and Communication Security Technology Center (ICST) has identified multiple denial-of-service (DoS) vulnerabilities in the Ing. Punzenberger COPA-DATA GmbH zenon human-machine interface (HMI) system.

ICS-CERT has coordinated with Ing. Punzenberger COPA-DATA GmbH, which has produced an updated software release that resolves these vulnerabilities. ICST has tested the new release and verified that it fully resolves these vulnerabilities.

AFFECTED PRODUCTS

The following product and version is affected:

- Ing. Punzenberger COPA-DATA GmbH zenon 6.51 SP0.

IMPACT

Successful exploitation of these vulnerabilities may allow an attacker to execute a DoS attack and potentially execute arbitrary code.

Impact to individual organizations depends on many factors that are unique to each organization. ICS-CERT recommends that organizations evaluate the impact of these vulnerabilities based on their operational environment, architecture, and product implementation.

BACKGROUND

According to Ing. Punzenberger COPA-DATA GmbH, zenon is an HMI that offers a graphical visualization system that runs entirely under Windows. The zenon product is used by companies worldwide for equipment automation in the automotive, energy and infrastructure, food and beverage, and pharmaceutical industries.

The Ing. Punzenberger COPA-DATA GmbH distribution network includes offices in Austria (for Central and Eastern Europe), France, Germany, Italy, Korea, Portugal and Spain, Sweden, the UK, and the USA.

VULNERABILITY CHARACTERIZATION

VULNERABILITY OVERVIEW

DENIAL OF SERVICE VULNERABILITY 1

A vulnerability exists that may allow an attacker to cause a DoS and possibly execute arbitrary code if the attacker sends a specially crafted packet to zenAdminSrv.exe on Port 50777/TCP.

The vendor has assigned Reference Number 25240 to the available update.

CVE-2011-4533[a] has been assigned to this vulnerability.

DENIAL OF SERVICE VULNERABILITY 2

A second vulnerability exists that could allow an attacker to crash the ZenSysSrv.exe service resulting in a DoS and possibly allow arbitrary code execution. This vulnerability can be exploited by connecting and disconnecting multiple times to the ZenSysSrv.exe service on Port 1101/TCP.

The vendor has assigned Reference Number 25212 to the available update.

CVE-2011-4534[b] has been assigned to this vulnerability.

VULNERABILITY DETAILS

EXPLOITABILITY

These vulnerabilities are remotely exploitable.

EXISTENCE OF EXPLOIT

No known exploits specifically target these vulnerabilities.

DIFFICULTY

An attacker with a low skill level can create the DoS; executing arbitrary code would require a more skilled attacker.

a. http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-4533, NIST uses this advisory to create the CVE website report. This website will be active sometime after publication of this advisory.
b. http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-4534, NIST uses this advisory to create the CVE website report. This website will be active sometime after publication of this advisory.

MITIGATION

Ing. Punzenberger COPA-DATA GmbH recommends that customers take the following actions in order to prevent successful exploitation of these vulnerabilities:

- Properly configure network access to Ports 1101/TCP and 50777/TCP.
- Disable the ZenSysSrv.exe service. This service should only be enabled when necessary and disabled immediately after being used.
- Install the Ing. Punzenberger COPA-DATA GmbH update. Customers can obtain the update for their systems from their local support source by referring to either Reference Number 25212 or 25240.

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.

The Control Systems Security Program (CSSP) also provides a section for control systems 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 reminds organizations to perform proper impact analysis and risk assessment prior to taking defensive measures.

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 February 06, 2012.

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 always provided to the vulnerability reporter unless the reporter notifies ICS-CERT that they wish to remain anonymous. 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 and the public at avoidable risk.