# ICS-CERT ADVISORY

## ICSA-12-018-02—CERTEC ATVISE SERVER REMOTE DOS

January 18, 2012

## OVERVIEW

Independent researcher Luigi Auriemma has identified a denial of service (DoS) vulnerability in Certec EDV GmbH atvise application. Certec has produced an update that resolves this vulnerability. Mr. Auriemma validated that the update resolves the vulnerability.

### AFFECTED PRODUCTS

Atvise versions older than Version 2.1 are affected.

### IMPACT

Successful exploitation of these vulnerabilities may allow an attacker to cause a DoS.

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

Certec EDV GmbH is an Austrian-based company.

The affected product, atvise, is web-based human-machine interface supervisory control and data acquisition (HMI SCADA) systems. According to Certec, atvise is deployed in every field of industrial automation. Certec states that these products are used worldwide.

## VULNERABILITY CHARACTERIZATION

### VULNERABILITY OVERVIEW

An attacker could exploit this vulnerability by sending specially crafted packets to Port 4840/TCP.

CVE-2011-4873[a] has been assigned to this vulnerability.

a. http://web nvd nist.gov/view/vuln/detail?vulnId=CVE-2012-4873, NIST uses this advisory to create the CVE website report. This website will be active sometime after publication of this advisory.

## 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 DoS.

## MITIGATION

Certec has developed a new version of atvise that prevents this DoS. Customers can download the new version of atvise at:

http://www.atvise.com.

Certc and ICS-CERT recommend that owners of vulnerable versions of the atvise product download and install the updated version as soon as possible.

ICS-CERT also 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.*[b] 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.

b. CSSP Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html, website last accessed January 17, 2012.

## 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 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.