



**American Water Works  
Association**

## Utility Member Benefit

**Government Affairs Office**  
1300 Eye Street NW  
Suite 701W  
Washington, DC 20005  
T 202.628.8303  
F 202.628.2846

**Headquarters**  
6666 West Quincy Avenue  
Denver, CO 80235-3098  
Washington, DC 20005  
T 303.794.7711  
F 303.795.1989  
[www.awwa.org](http://www.awwa.org)

The Authoritative Resource for Safe Water<sup>®</sup>

---

## Security Alert

**TO: AWWA Member Utilities**  
**FROM: AWWA Government Affairs**  
**DATE: October 26, 2010**

<b>Who:</b>	<b>Water utility/Information technology managers</b>
<b>What:</b>	<b>VTScada software vulnerability</b>
<b>Action:</b>	<b>See attached recommendations from ICS-CERT</b>

Water utility managers and information technology staff should be aware of a potential security vulnerability related to VTScada software. Details and recommendations are included in the advisory below from the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), part of the U.S. Department of Homeland Security.

ICS-CERT is part of the broader US-CERT, which is charged with providing response support and defense against cyber attacks for the Federal Civil Executive Branch and information sharing and collaboration with state and local government, industry and international partners.

Questions can be directed to Kevin Morley, AWWA security & preparedness program manager, at [kmorley@awwa.org](mailto:kmorley@awwa.org), 202-326-6124.



# ICS-CERT

INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

## ICS-CERT ALERT

ICS-ALERT-10-299-01 - TRIHEDRAL VTSCADA & VTS INTERNET SERVER ACCESSABILITY  
October 26, 2010

### ALERT

#### SUMMARY

ICS-CERT has received reports from an independent security researcher who used the SHODAN search engine to discover that some installations of the Trihedral VTScada and VTS Internet Server system are directly accessible from the Internet and are using potentially insecure mechanisms for authentication and authorization. Some of these systems were found to be configured with a VTScada default user name and password.

VTScada is HMI software designed for the water and wastewater industry. The software product provides remote asset management features to VTS telemetry applications. Use of VTScada can range from stand-alone workstation applications to unified county-wide systems that tie plants and SCADA centrals together. Approximately 66% of VTScada installations are in the United States. VTScada provides an optional component called VTS Internet Server, which can be configured to allow remote access using an ActiveX plug-in.

ICS-CERT published Control Systems Analysis Report “CSAR-10-025-01 Analysis of Shodan – Computer Search Engine,” (attached) which discusses the importance of minimizing network exposure by ensuring that control system devices are not visible on the Internet. Control System owners and operators are also advised to audit systems for the use of default user names and passwords.

#### VULNERABLE CONFIGURATION

Organizations with VTScada installed should understand that a minimum of two deliberate actions would have to be performed to allow this security breach.

1. The server would need to be configured to allow remote user connections. This is not unusual and the VTScada manual is clear about the security risks associated with this action.
2. The default user account “Manager1” would have to exist with the default password. The VTScada documentation recommends that users delete the default Manager1 user account and also change the default password.

#### RECOMMENDATIONS

ICS-CERT recommends:

- Placing all control systems assets behind firewalls, separated from the business network
- Deploying secure remote access methods such as Virtual Private Networks (VPNs) for remote access
- Removing, disabling, or renaming any default system accounts (where possible)
- Requiring the use of strong passwords (<http://csrc.nist.gov/publications/drafts/800-118/draft-sp800-118.pdf>).



# ICS-CERT

INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

---

Please report any issues affecting control systems in critical infrastructure environments to ICS-CERT.

ICS-CERT Operations Center

1-877-776-7585

[www.ics-cert.org](http://www.ics-cert.org)

[ICS-CERT@DHS.GOV](mailto:ICS-CERT@DHS.GOV)

***What is an ICS-CERT Alert?*** An ICS-CERT Alert is intended to provide timely notification to critical infrastructure owners and operators concerning threats or activity with the potential to impact critical infrastructure computing networks.