Remote access of your system - a look at security best practices.

A preliminary response to the alleged cyber-attack on a water treatment plant in Oldsmar, Florida.

A headline recently appeared in media outlets in the USA regarding what appears to have been a cyber-attack on a water treatment plant in Oldsmar, Florida. The articles reported that an operator witnessed their cursor being moved around the screen, by what was considered to be an unknown entity and that setpoints were being changed to potentially toxic levels on the chemical dosage in one part of the treatment process. The alert operator quickly changed these levels back to within safe levels. In a statement reported in the Tampa Bay Times, Oldsmar Mayor Eric Seidel said, "The protocols that we have in place, monitoring protocols, they work - that's the good news. Even had they not caught them, there's redundancies in the system that would have caught the change in the pH level." He went on to say, "The important thing is to put everyone on notice. There's a bad actor out there."

Our Response

This case is being fully investigated by the authorities so we at Trihedral are not going to comment further on what allegedly took place. However, we would like to point out some best practice measures that should be considered when allowing remote control of any control system software.

This was NOT a VTScada System

It appears that the utility's SCADA software was not directly compromised. According to reports, the utility was using third-party software that allows users outside their firewall to 'take over' and control internal computers. It appears that the assailant used this product to access and operate the SCADA application.

VTScada systems use our own dedicated Thin Clients as a means of secure, remote monitoring and/or control of systems. Strong passwords are universally recommended. VTScada includes tools to enforce these and other security best practices. We have over 34 years of experience keeping our systems secure and providing our customers with best practice strategies to allow safe, secure local and remote access.

Should I not have any remote access to my control system?

That really depends on many factors. There are significant advantages in being able to remotely access your system. Speed or reaction time is one of them. Think of this scenario: You could only do something physically at a remote site, and someone obtained the keys to it and gained entry. Perhaps they make some destructive changes to the system, opening valves, turning on/off pumps, changing dosage levels. How long would it take before you would even notice that something critical had changed and more importantly, how long before you could get to the site to make a corrective change?

Security must be looked at across the entire system

As the world realizes that critical infrastructure is indeed "critical," all bodies need to assume that someone, somewhere may try to launch an attack for whatever reason. This could be from within an organization or indeed externally. The "I'll just keep the system off the internet" approach is not a sustainable argument. This is akin to saying, my house is burglar proof. That's probably not the case unfortunately. It may be extremely strong to prevent someone crashing through the walls or windows but what if someone living there leaves the key under the mat or forgets to lock the door? That concept will likely be tested.

Bad Actors pose in many forms

The question is, how do you put measures in place to stop them intruding your system and, if you can't prevent them, how do you stop them from wreaking havoc on the inside once they've gained entry? This is where good planning is key. You really need to examine all these items...

- Intrusion prevention (both physical and electronic)
- System access control
- Moving target defense adoption
- Password strategy
- Staff training and compliance
- Operational policy and safeguards
- System redundancy

www.trihedral.com 1.800.463.2783 (North America) 1.902.835.1575 (Worldwide)
info@trihedral.com +44 (0) 1224 258910 (UK) 1.403.805.1972 (Western Canada)

Keep your OS and SCADA software up to date

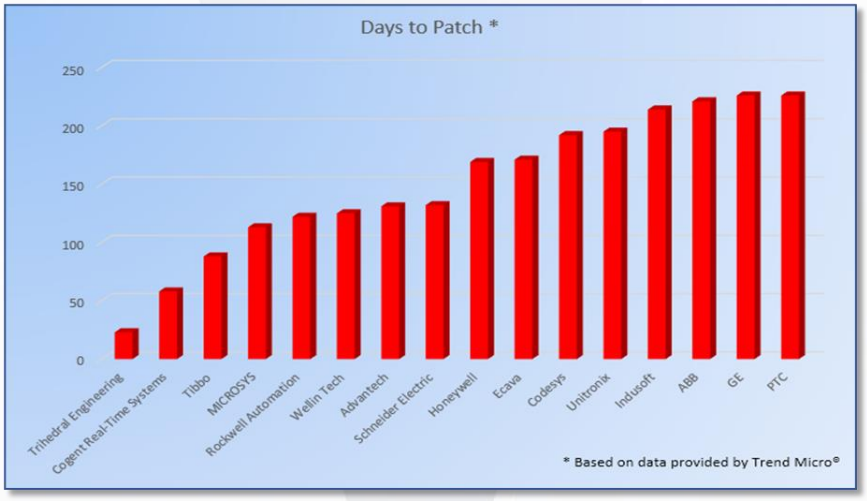
It is always important to stay up to date with your SCADA and operating system software, as the world is continuously changing, with would-be hackers attempting to find new ways to circumvent security measures.

Vendor response time to known issues

An aspect that is often ignored is how long it takes vendors to patch security vulnerabilities found in their SCADA platforms.

ICS-CERT is a US government agency that continuously tests for vulnerabilities in control system software used in critical-infrastructure. When a potential vulnerability is identified, they contact the vendor who then is given a period of time to develop and distribute the fix before the issue is made public.

The chart below, provided by Trend Micro, shows how long it takes major software vendors to patch these vulnerabilities once they are notified. In many cases, the announcement is made public before the vendors have gotten around to addressing the issue. Thankfully, Trihedral Engineering (that's VTScada), was identified as having the shortest time to patch vulnerabilities.



Days to Patch Security Issues Following Notification by ICS-CERT

Data based on this 2017 research paper: https://documents.trendmicro.com/assets/wp/wp-hacker-machine-interface.pdf

Additional resources

VTScada Security Best Practices

https://www.vtscada.com/help/Content/D_Customize/Dev_SecurityBestPractices.htm

Integrated VTScada tools to support your security strategy

- Centralized account management
- Industry-standard encryption (TLS)
- Read Only Server Options
- Windows active directory support
- Immediate application-wide change deployment

VTScada implementations are current and compliant with…

- NERC/CIP (North American Electric Reliability Corporation)
- DFARS 252 (Defense Federal Acquisition Regulations Supplement)
- NIST 800 (National Institute of Standards and Technology)
- Marine reliability standards ABS, Lloyds Bureau, DNV, BV

We are here to help

We are happy to discuss any security concerns that you may have regarding your system, whether it is our SCADA software or not. Contact: info@trihedral.com