Compromise of U.S. Water Treatment Facility

us-cert.cisa.gov/ncas/alerts/aa21-042a

Summary

On February 5, 2021, unidentified cyber actors obtained unauthorized access to the supervisory control and data acquisition (SCADA) system at a U.S. drinking water treatment facility. The unidentified actors used the SCADA system's software to increase the amount of sodium hydroxide, also known as lye, a caustic chemical, as part of the water treatment process. Water treatment plant personnel immediately noticed the change in dosing amounts and corrected the issue before the SCADA system's software detected the manipulation and alarmed due to the unauthorized change. As a result, the water treatment process remained unaffected and continued to operate as normal. The cyber actors likely accessed the system by exploiting cybersecurity weaknesses, including poor password security, and an outdated operating system. Early information indicates it is possible that a desktop sharing software, such as TeamViewer, may have been used to gain unauthorized access to the system, although this cannot be confirmed at present date. Onsite response to the incident included Pinellas County Sheriff Office (PCSO), U.S. Secret Service (USSS), and the Federal Bureau of Investigation (FBI).

The FBI, the Cybersecurity and Infrastructure Security Agency (CISA), the Environmental Protection Agency (EPA), and the Multi-State Information Sharing and Analysis Center (MS-ISAC) have observed cyber criminals targeting and exploiting desktop sharing software and computer networks running operating systems with end of life status to gain unauthorized access to systems. Desktop sharing software, which has multiple legitimate uses—such as enabling telework, remote technical support, and file transfers—can also be exploited through malicious actors' use of social engineering tactics and other illicit measures. Windows 7 will become more susceptible to exploitation due to lack of security updates and the discovery of new vulnerabilities. Microsoft and other industry professionals strongly recommend upgrading computer systems to an actively supported operating system. Continuing to use any operating system within an enterprise beyond the end of life status may provide cyber criminals access into computer systems.

Click here for a PDF version of this report.

Technical Details

Desktop Sharing Software

The FBI, CISA, EPA, and MS-ISAC have observed corrupt insiders and outside cyber actors using desktop sharing software to victimize targets in a range of organizations, including those in the critical infrastructure sectors. In addition to adjusting system operations, cyber

actors also use the following techniques:

- Use access granted by desktop sharing software to perform fraudulent wire transfers.
- Inject malicious code that allows the cyber actors to
    - Hide desktop sharing software windows,
    - Protect malicious files from being detected, and
    - Control desktop sharing software startup parameters to obfuscate their activity.
- Move laterally across a network to increase the scope of activity.

TeamViewer, a desktop sharing software, is a legitimate popular tool that has been exploited by cyber actors engaged in targeted social engineering attacks, as well as large scale, indiscriminate phishing campaigns. Desktop sharing software can also be used by employees with vindictive and/or larcenous motivations against employers.

Beyond its legitimate uses, when proper security measures aren't followed, remote access tools may be used to exercise remote control over computer systems and drop files onto victim computers, making it functionally similar to Remote Access Trojans (RATs). TeamViewer's legitimate use, however, makes anomalous activity less suspicious to end users and system administrators compared to RATs.

Windows 7 End of Life

On January 14, 2020, Microsoft ended support for the Windows 7 operating system, which includes security updates and technical support unless certain customers purchased an Extended Security Update (ESU) plan. The ESU plan is paid per-device and available for Windows 7 Professional and Enterprise versions, with an increasing price the longer a customer continues use. Microsoft will only offer the ESU plan until January 2023. Continued use of Windows 7 increases the risk of cyber actor exploitation of a computer system.

Cyber actors continue to find entry points into legacy Windows operating systems and leverage Remote Desktop Protocol (RDP) exploits. Microsoft released an emergency patch for its older operating systems, including Windows 7, after an information security researcher discovered an RDP vulnerability in May 2019. Since the end of July 2019, malicious RDP activity has increased with the development of a working commercial exploit for the vulnerability. Cyber actors often use misconfigured or improperly secured RDP access controls to conduct cyberattacks. The xDedic Marketplace, taken down by law enforcement in 2019, flourished by compromising RDP vulnerabilities around the world.

Mitigations

General Recommendations

The following cyber hygiene measures may help protect against the aforementioned scheme:

- Update to the latest version of the operating system (e.g., Windows 10).
- Use multiple-factor authentication.
- Use strong passwords to protect Remote Desktop Protocol (RDP) credentials.
- Ensure anti-virus, spam filters, and firewalls are up to date, properly configured, and secure.
- Audit network configurations and isolate computer systems that cannot be updated.
- Audit your network for systems using RDP, closing unused RDP ports, applying multiple-factor authentication wherever possible, and logging RDP login attempts.
- Audit logs for all remote connection protocols.
- Train users to identify and report attempts at social engineering.
- Identify and suspend access of users exhibiting unusual activity.

Water and Wastewater Systems Security Recommendations

The following physical security measures serve as additional protective measures:

- Install independent cyber-physical safety systems. These are systems that physically prevent dangerous conditions from occurring if the control system is compromised by a threat actor.
- Examples of cyber-physical safety system controls include:
    - Size of the chemical pump
    - Size of the chemical reservoir
    - Gearing on valves
    - Pressure switches, etc.

The benefit of these types of controls in the water sector is that smaller systems, with limited cybersecurity capability, can assess their system from a worst-case scenario. The operators can take physical steps to limit the damage. If, for example, cyber actors gain control of a sodium hydroxide pump, they will be unable to raise the pH to dangerous levels.

Remote Control Software Recommendations

For a more secured implementation of TeamViewer software:

- Do not use unattended access features, such as “Start TeamViewer with Windows” and “Grant easy access.”
- Configure TeamViewer service to “manual start,” so that the application and associated background services are stopped when not in use.
- Set random passwords to generate 10-character alphanumeric passwords.
- If using personal passwords, utilize complex rotating passwords of varying lengths. Note: TeamViewer allows users to change connection passwords for each new session. If an end user chooses this option, never save connection passwords as an option as they can be leveraged for persistence.

- When configuring access control for a host, utilize custom settings to tier the access a remote party may attempt to acquire.
- Require remote party to receive confirmation from the host to gain any access other than “view only.” Doing so will ensure that, if an unauthorized party is able to connect via TeamViewer, they will only see a locked screen and will not have keyboard control.
- Utilize the ‘Block and Allow’ list which enables a user to control which other organizational users of TeamViewer may request access to the system. This list can also be used to block users suspected of unauthorized access.

Contact Information

To report suspicious or criminal activity related to information found in this Joint Cybersecurity Advisory, contact your local FBI field office at www.fbi.gov/contact-us/field, or the FBI’s 24/7 Cyber Watch (CyWatch) at (855) 292-3937 or by e-mail at CyWatch@fbi.gov or your local WMD Coordinator. When available, please include the following information regarding the incident: date, time, and location of the incident; type of activity; number of people affected; type of equipment used for the activity; the name of the submitting company or organization; and a designated point of contact.

To request incident response resources or technical assistance related to these threats, contact CISA at Central@cisa.dhs.gov.

Revisions

February 11, 2021: Initial Version

February 12, 2021: Update to PDF File

This product is provided subject to this Notification and this Privacy & Use policy.