

STATE OF CONNECTICUT

DEPARTMENT OF PUBLIC HEALTH

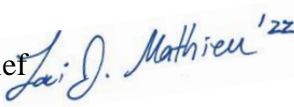


Manisha Juthani, MD
Commissioner

Ned Lamont
Governor
Susan Bysiewicz
Lt. Governor

ENVIRONMENTAL HEALTH AND DRINKING WATER BRANCH

DWS Circular Letter# 2022- 26

TO: Community Public Water Systems
FROM: Lori Mathieu, Public Health Branch Chief 
DATE: May 27, 2022
SUBJECT: Joint Cybersecurity Advisory: Weak Security Controls and Practices Routinely Exploited for Initial Access

The Department of Public Health (DPH) Drinking Water Section (DWS) is alerting the Community Water Systems regarding a joint Cybersecurity Advisory published by the Cybersecurity and Infrastructure Security Agency ([CISA](#)) that identifies commonly exploited controls and practices used by cyber actors to gain initial access or as part of other tactics to compromise a victims' system

In partnership with the Federal Bureau of Investigation ([FBI](#)), National Security Agency ([NSA](#)), and international partners from the Canadian Centre for Cyber Security ([CCCS](#)), New Zealand National Cyber Security Centre ([NZ NCSC](#)), Computer Emergency Response Team New Zealand ([CERT-NZ](#)), Netherlands National Cyber Security Centre ([NCSC-NL](#)), and United Kingdom's National Cyber Security Centre ([NCSC-UK](#)) it includes best practices to mitigate the malicious tactics and weaknesses.

The CSA, "[Weak Security Controls and Practices Routinely Exploited for Initial Access](#)", provides several recommendations and technical details that organizations can take to reduce their risk of becoming a victim to malicious cyber activity, such as:

- **Control access**, including adopt a zero-trust security model that eliminates implicit trust in any one element, node, or service, and control who has access to your data and services.
- **Implement credential hardening**, including apply multifactor authentication (MFA) on all virtual private network (VPN) connections, external-facing services, and privileged accounts.
- **Establish centralized log management**, including ensure that each application and system generates sufficient log information.



Phone: (860) 509-7333 • Fax: (860) 509-7359
Telecommunications Relay Service 7-1-1
410 Capitol Avenue, P.O. Box 340308
Hartford, Connecticut 06134-0308
www.ct.gov/dph

Affirmative Action/Equal Opportunity Employer



- **Employ antivirus programs**, including monitor antivirus scan results on a routine basis.
- **Use detection tools and search for vulnerabilities**, including implement endpoint and detection response tools.
- **Maintain rigorous configuration management programs**, including always operate services exposed on internet-accessible hosts with secure configuration.
- **Initiate a software and patch management program**, including prioritize patching known exploited vulnerabilities.

Along with our interagency and international partners, DPH Drinking Water Section encourages all organizations to review the advisory for more details on the malicious actors' commonly used techniques for initial access, recommended practices, and apply the recommended mitigations in this [advisory](#).

In addition, we encourage all organizations to review CISA's [Shields Up webpage](#) to find recommended guidance and actions for all organizations, corporate leaders and CEOs, steps to protect yourself and your family, and a technical webpage with guidance from CISA and Joint Cyber Defense Collaborative (JCDC) industry partners.

The Department of Public Health encourages all water systems to report malicious or suspicious activities to [CISA](#) and/or the FBI via your [local FBI field office](#) or the FBI's 24/7 CyWatch at (855) 292-3937 or CyWatch@fbi.gov.

c. Deputy Commissioner Heather Aaron, MPH, LNHA, Department of Public Health