FREE CYBER VULNERABILITY SCANNING FOR WATER UTILITIES

WATER SECTOR COORDINATING COUNCIL

OVERVIEW

Drinking water and wastewater systems are an essential community lifeline. It is important to protect your system from cyberattacks to maintain its vital operations. You can reduce the risk of a cyberattack at your utility by externally scanning your networks for vulnerabilities caused by publicly facing devices. The Cybersecurity and Infrastructure Security Agency (CISA) can help your drinking water and wastewater system identify and address vulnerabilities with a no cost vulnerability scanning service subscription. CISA, the Water Sector Coordinating Council, and the Association of State Drinking Water Administrators encourage drinking water and wastewater utilities to use this service.

BENEFITS

CISA's vulnerability scanning can help your utility identify and address cybersecurity weaknesses that an attacker could use to impact your system. The benefits of this service include:

- Identifying internet-accessible assets
- Identifying vulnerabilities in your utility's assets connected to the internet, including Known Exploited Vulnerabilities and internet-exposed services commonly used for initial access by threat actors and some ransomware gangs
- Weekly reports on scanning status and recommendations for mitigating identified vulnerabilities
- Significant reduction in identified vulnerabilities in the first few months of scanning for newly enrolled water utilities
- Ongoing detection and reporting with continuous scanning for new vulnerabilities

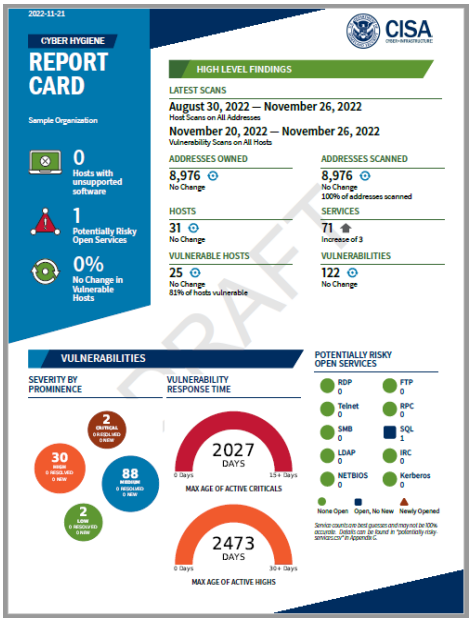

Figure 1: Sample Page in Weekly Report

HOW DOES IT WORK?

CISA uses automated tools to conduct vulnerability scanning on your external networks. These tools look for vulnerabilities and weak configurations that adversaries could use to conduct a cyberattack. CISA's scanning provides an

external, non-intrusive review of internet-accessible systems. The scanning does not reach your private network and cannot make any changes. CISA will send you weekly reports with information on known vulnerabilities found on your internet-accessible assets, week-to-week comparisons, and recommended mitigations. Figure 1 shows an example of the Report Card included in the weekly report. You will also receive ad-hoc alerts for any urgent findings.

CISA does not share any attributable information without written and agreed consent from the stakeholder. CISA summarizes aggregate, anonymized data to develop non-attributable reports for analysis purposes. Figure 2 summarizes the phases in CISA's vulnerability scanning enrollment.

Pre-Planning	Planning	Execution	Reporting
Stakeholder: • Requests vulnerability scanning service • Signs and returns documents	**Stakeholder:** • Provides target list (scope)	**CISA:** • Performs initial scan of submitted scope • Rescans stakeholder's target list at the following intervals based on highest severity of identified vulnerabilities: ⇒ 12 hours for "critical" and "known exploited" ⇒ 24 hours for "high" ⇒ 4 days for "medium" ⇒ 6 days for "low" ⇒ 7 days for "no vulnerabilities"	**CISA:** • Sends ad-hoc alerts within 24 hours of detecting a new "urgent" finding • Delivers weekly report to stakeholder • Provides detailed findings in consumable format to stakeholder • Provides vulnerability mitigation recommendations to stakeholder

Figure 2: Phases of Vulnerability Scanning Enrollment

HOW CAN I GET STARTED?

1. Email vulnerability@cisa.dhs.gov with the subject line "Requesting Vulnerability Scanning Services." Include the name of your utility, a point of contact with an email address, and the physical address of your utility's headquarters.
2. CISA will reply with a Service Request Form and Vulnerability Scanning Acceptance Letter to obtain the necessary information about your utility and your authorization to scan your public networks.
3. Scanning typically begins within 10 days of receiving all completed forms.

WHO CAN I CONTACT WITH QUESTIONS ABOUT VULNERABILITY SCANNING?

Reach out to us at vulnerability@cisa.dhs.gov.

WHERE CAN I GET ADDITIONAL CYBERSECURITY RESOURCES?

CISA, the Environmental Protection Agency (EPA), and water sector partners have developed numerous tools and resources that water utilities can use to increase their cybersecurity. Visit:

- CISA: cisa.gov/water
- EPA: https://www.epa.gov/waterriskassessment/epa-cybersecurity-water-sector
- Water Information Sharing and Analysis Center (WaterISAC): waterisac.org
- American Water Works Association: awwa.org/cybersecurity