STATE OF CONNECTICUT

DEPARTMENT OF PUBLIC HEALTH

Manisha Juthani, MD
Commissioner

Ned Lamont
Governor

Susan Bysiewicz
Lt. Governor

DATE: December 18, 2023 OPHPR-2023-015

TO: Hospital Emergency Managers
Local Health Directors

FROM: Francesca Provenzano, MPH, RS
Chief, Public Health Preparedness and Response Section

SUBJECT: Cyber Security Resources

On Friday, December 15, 2023, the DPH Public Health Preparedness and Response Section received the following communication from ASPR Region 1 concerning cyber security resources available through the Cybersecurity and Infrastructure Security Agency. Please feel free to share this communication with your partners as you feel appropriate.

> Today, the Cybersecurity and Infrastructure Security Agency (CISA) published a cybersecurity advisory (CSA), Enhancing Cyber Resilience: Insights from the CISA Healthcare and Public Health Sector Risk and Vulnerability Assessment, detailing the agency's key findings and activities during a Risk and Vulnerability Assessment (RVA) conducted at a healthcare and public health (HPH) organization in early 2023. The advisory also provides network defenders and software manufacturers recommendations for improving their organizations and customers' cyber posture, which reduces the impact of follow-on activity after initial access.
>
> The CISA assessments team identified several findings as potentially exploitable vulnerabilities that could compromise the confidentiality, integrity, and availability of the tested environment. Tailored for HPH organizations of all sizes as well as for all critical infrastructure organizations, the advisory provides several recommended mitigations mapped to 16 specific cybersecurity weaknesses identified during the RVA. Also, the advisory provides three mitigation strategies that all organizations should implement: (1) Asset management and security, (2) Identity management and device security, and (3) Vulnerability, patch, and configuration management. Each strategy has specific focus areas with details and steps on how HPH entities can implement them to strengthen their cybersecurity posture.

This advisory builds on the CISA and Health and Human Services Healthcare and Public Health Cybersecurity Toolkit and CISA's Mitigation Guide for HPH Sector that were recently released. The recommended mitigations for network defenders are mapped to the Cross-Sector Cybersecurity Performance Goals (CPGs).

The recommended actions for software manufacturers are aligned to the recently updated, Principles and Approaches for Secure by Design Software, a joint guide co-sealed by 18 U.S. and international agencies. It urges software manufacturers to take urgent steps necessary to design, develop, and deliver products that are secure by design.

All HPH sector and other critical infrastructure organizations deploying on-premises software, as well as software manufacturers, are encouraged to apply the recommended mitigations to harden networks against malicious activity and to reduce the likelihood of domain compromise.

For more information and resources, HPH entities can visit CISA's Healthcare and Public Health Cybersecurity Toolkit and Healthcare and Public Health Sector webpages.

Regards,

CISA Region 1 – New England