CISA INSIGHTS

JANUARY 2021

Cybersecurity Perspectives:
Healthcare and Public Health Response to COVID-19

THREATS TO THE HEALTHCARE AND PUBLIC HEALTH (HPH) SECTOR

Disruptive ransomware and other malicious cyber attacks significantly reduce HPH entities' ability to provide patient care and can contribute to patient mortality. Threat actors aim to disrupt HPH entities who have a low tolerance for down-time and may be experiencing resource and staffing constraints due to the COVID-19 pandemic.

CISA recommends that all HPH entities review the following observations and findings, which are derived from an analysis of HPH entities enrolled in CISA's free vulnerability scanning service from March to October 2020, and take appropriate action to reduce potential vulnerability and maintain resilient cybersecurity practices. Email vulnerability_info@cisa.dhs.gov to sign up for free CISA Cyber Hygiene Services.

CONCERNS	Threat actors are leveraging internet-facing risky ports and services (e.g. RDP) to establish initial access to networks and deliver ransomware	Cyber threat actors are chaining critical vulnerabilities on perimeter devices with newer vulnerabilities to compromise networks and escalate	Unsupported software and operating systems (OS) are being used on internet-facing assets, leaving systems vulnerable to widely known exploits
FINDINGS MAR TO OCT 2020	**49%** of enrolled HPH entities had risky ports and services exposed on internet-facing assets	Recent chaining attacks are exploiting unpatched Virtual Private Network (VPN) and perimeter device vulnerabilities	**58%** of enrolled HPH entities were using unsupported legacy or end-of-life software and OS
TARGETED MITIGATIONS	**Restrict internet-facing risky services** • Limit exposure by disabling or securely configuring (e.g. enable multi-factor authentication and encryption risky services such as: — RDP — SMB — Telnet — DICOM • Perform cost-benefit analysis of existing risky services exposed to the internet	**Maintain diligent mission critical patching** • Patch actively exploited vulnerabilities first • Review vulnerability backlogs and patch legacy CVEs that may be used in chaining attacks • Triage then apply patches and software updates on systems supporting hospital operations and patient care • Implement compensating controls or adjust security architecture to mitigate risk when patching is not possible	**Secure/retire legacy systems** • Isolate and segment legacy systems to prevent lateral movement • Upgrade or replace unsupported legacy software and OS • Maintain accurate hardware and software inventory

BASELINE PREPARATION FOR LIKELY ATTACKS

- Maintain backups in secure offline environments and regularly test backups
- Filter emails with known malicious indicators at the email gateway
- Monitor network for malcious activity and signs of attack
- Focus phishing training on current events and reporting suspicious activity
- Implement and test cyber incident response plans

ADDITIONAL RESOURCES

- CISA and MS-ISAC Joint Ransomware Guide and CISA, FBI, and HHS Joint HPH Cybersecurity Advisory
- Health Sector Coordinating Council (HSCC) and HHS Health Industry Cybersecurity Practices
- Health Sector Cybersecurity Coordination Center (HC3) and Health Information Sharing and Analysis Center (H-ISAC)

PLEASE SHARE YOUR THOUGHTS. WE RECENTLY UPDATED OUR ANONYMOUS **PRODUCT SURVEY**; WE'D WELCOME YOUR FEEDBACK.