UETN Vulnerability Management Procedure for Telehealth

UETN conducts vulnerability scans of all systems connected to its network that supports the delivery of healthcare systems and services for member sites. This procedure, focused on Critical vulnerabilities, is intended to encourage member sites to address vulnerabilities within a defined timeframe.

Definitions

Vulnerability: A weakness by which an intruder can easily gain control of a device, which can lead to the compromise of a site's entire network security. Any device that uses an IP address is vulnerable to being exploited. Vulnerabilities are rated on a scale of Info, Low, Medium, High and Critical.

Critical vulnerability: The most severe vulnerability with the greatest risk of exploitation of a network. For example, vulnerabilities at this level may include full read and write access to files, remote execution of commands, and the presence of backdoors.

Open vulnerability: An identified Critical vulnerability that has not been addressed.

Closed vulnerability: An identified Critical vulnerability that has been addressed by either 1) fixing the problem if feasible, or 2) through documentation if not.

Device: A computer, phone, tablet, printer or other machine that uses an IP address to connect into a network.

Communication Plan

1. Vulnerability scans occur weekly and reported weekly. All communication with site technical contacts is managed through an issue tracking program (Jira).
2. Notifications of new issues designated as Critical and a summary of all open Critical vulnerabilities are provided to site technical contacts weekly.
3. Site technical contacts are required to document when a Critical vulnerability cannot be corrected, such as one that required manufacturer intervention (a software upgrade, which they may/may not be willing to do) or replacement of capital equipment, which may be unrealistic. Once documented, these vulnerabilities will be removed from reporting for up to six month increments, at which time a review and documentation update is required.
4. UETN will:
    a. provide documentation templates for optional use by site IT staff to assist with this process.
    b. provide reports as requested by sites for use in security audits.
    c. host weekly office hours to provide support for vulnerabilities

Procedure

1. Sanctions for unresolved issues effecting the network will be imposed once a month following the last scan of the month.
2. Devices will be blocked when they have one or more Critical vulnerabilities open for 8 weeks or more as of the last scan of a month.
    a. The device will remain blocked until the vulnerabilities are addressed.
    b. Exceptions will be made for devices directly impacting patient care.
    c. Extensions may be requested via documentation.

3. If a site has one or more Critical vulnerabilities open for 16 weeks or more and has closed less than 90% of its Critical vulnerabilities as of the last scan of a month, it will be remediated by UETN leadership, up to and including suspension of network participation.

Board Action
Adopted February 2016
Revised and reaffirmed August 2021