PCI DSS Vulnerability Scanning Standard for University of Tennessee and University of Tennessee Foundation Merchants

Revision: March 28, 2016

Purpose

To outline the key roles and responsibilities, requirements, and notification methods when network vulnerability scanning is required by the Payment Card Industry Data Security Standards (PCI DSS).

Scope

This standard applies to all University of Tennessee system-wide merchants and all University of Tennessee Foundation merchants who are completing PCI DSS Self-Assessment Questionnaire (SAQ) A-EP, SAQ B-IP, SAQ C, or SAQ D.

Key Roles and Responsibilities

Merchant

- Works with the campus CIO/ISO to define the specific scope for that merchant by providing list of all systems used for processing credit cards.
- Notifies campus CIO/ISO when there is any change to the list of systems.
- Ensures that all hosts to be scanned are turned on and not in sleep or hibernate mode before the agreed upon date and time.

Campus Chief Information Officer/Information Security Officer

- Maintains up-to-date list of all systems used for processing credit cards.
- Maintains CDE for that campus.
- Maintains segmentation controls and methods documentation.
- Provides UTSA ISO with current list of all systems to be scanned.
- Provides UTSA ISO access to the CDE for purposes of internal scanning.
- Notifies UTSA ISO in the event of any significant change in the network.

University of Tennessee System Administration Information Security Office (UTSA ISO)

- Performs the internal scans.
- Works with Qualys, the ASV, to perform the external scans.
- Provides notification of internal and external scan results.
- Maintains the *PCI DSS Vulnerability Scanning Standard for University of Tennessee and University of Tennessee Foundation Merchants*.

Vulnerability Scanning Requirements for PCI v3.x

PCI DSS Requirement 11.2, and its sub-requirements, requires vulnerability scanning to validate that PCI systems are free from "high-risk" vulnerabilities. Risk rankings, a part of PCI DSS Requirement 6.1, are based on industry best practices, as well as consideration of potential impact. Criteria for ranking vulnerabilities may include consideration of the CVSS base score, and/or the classification by the vendor, and/or type of systems affected.

Any vulnerability that is considered "High," and/or is designated a severity level 3, 4, or 5, and/or has a CVSS base score of 4.0 or higher must be remediated at once. Systems such as security systems, public-facing devices and systems, and databases, as well as those systems that store, process, or transmit cardholder data are considered critical systems and must be remediated at once.

All scans, both internal and external, will follow these guidelines:

- Vulnerability scans must be performed at least quarterly.
- Vulnerability scans must be performed after any significant change in the network (i.e., new system components added to the CDE, changes in network topology, firewall rule modifications, product upgrades).
- All hosts subjected to vulnerability scans must be powered on and not in sleep/hibernate mode.
- All hosts subjected to vulnerability scans must pass each scan.
- Remediation must be done immediately and scans will be repeated until all hosts pass.
- Scans must be non-disruptive and must not include denial of service (DoS) or buffer overflow attacks.
- Scans must include a host discovery element that searches the network for live hosts.
- Scans must include a service discovery element that includes both TCP and UDP port scans on all live hosts.
- OS and service fingerprinting must take place to identify the operating characteristics of live hosts.

The internal vulnerability scan process will follow these guidelines:

- The UTSA ISO will put scans on merchants' IT staff calendars for the regularly agreed upon date and time.
- The UTSA ISO will remind the campus network group and CIO/ISO each month before scans are to be run.
- The UTSA ISO will perform the internal vulnerability scans.
- The UTSA ISO will be given access to the CDE via firewall rules.

The external vulnerability scan process will follow these guidelines:

- The UTSA ISO performs scans at 10:00am on the second Wednesday of the second month of each quarter and will keep the scan on merchants' IT staff calendars.
- The UTSA ISO will remind the campus network group and CIO/ISO each quarter before scans are to be run.
- The external scans are performed by Qualys, a certified ASV.
- All hosts subjected to external scans must pass each quarterly scan. If only one hosts fails the scan, it will cause ALL hosts (including hosts for all other UT merchants) to fail until remediation has been completed.

Notification

The UTSA ISO will notify the merchant and campus CIO/ISO immediately in the event vulnerabilities are identified. The scan results will be forwarded to the merchant and campus CIO/ISO via secure email. These scan results contain potential solutions and/or workarounds for any vulnerability found in the scan.

The UTSA ISO provides official reporting to the Treasurer's Office, campus Chief Business Officer, campus CIO/ISO, University of Tennessee Foundation Assistant Vice President of Finance and Operations, and merchant. While the internal scan does not require official reporting, official notification will be sent when remediation is not done. The external vulnerability scanning report shall include the following:

- Letter certifying compliant status with regards to external vulnerability scan
- Executive Summary (to the Treasurer's Office and CBO)

Definitions

- Approved Scanning Vendor (ASV) – An ASV is a company approved by the PCI SSC to conduct external vulnerability scans.
- Cardholder – The customer to whom a payment card is issued or an individual authorized to use the payment card is known as the cardholder.
- Cardholder Data (CHD) – Cardholder data is any personally identifiable data associated with a cardholder's account. At a minimum, CHD consists of the full primary account number (PAN), but may also consist of the full PAN plus any of the following: cardholder name, expiration date, and/or service code.
- Cardholder Data Environment (CDE) – The cardholder data environment consists of the people, processes, and technology that store, process, or transmit cardholder data or sensitive authentication data, including any connected system components.
- Common Vulnerability Scoring System (CVSS) – CVSS is a vendor agnostic, industry open standard designed to convey the severity of computer security vulnerabilities and help determine the urgency and priority of response.
- Host – Main computer hardware on which computer software is resident.

- Network Segmentation – Network segmentation isolates system components that store, process, or transmit cardholder data from systems that do not.
- UT or UTFI Merchant – A UT or UTFI department/office/organization that collects payments, electronically or manually, via payment card OR is otherwise involved in storing, processing, transmitting, or receiving payment card or cardholder data.
- Vulnerability – A vulnerability is a weakness in a system that can result in a compromise or data breach.
- Vulnerability Scan – A vulnerability scan is a process by which a merchant's systems are remotely checked for vulnerabilities through use of scanning tools. Scans may identify vulnerabilities in operating systems, services, and devices that could be used by malicious individuals.