Vulnerability Management

Standard ID
IOT-CS-SEC-108

Published Date
3/15/2006

Effective Date
3/15/2006

Last Updated
5/19/2017

Next Review Date
5/19/2018

Policy
13.0 Security Continuous Monitoring (DE.CM)
   13.8 DE.CM-8
       13.8.1 Vulnerability Scanning

Purpose
This Standard prescribes vulnerability management requirements to ensure devices are protected from software vulnerabilities.

Scope
All Devices that Connect to the State Network

Statement
IOT will follow the steps outlined below to manage vulnerabilities on devices for which they are responsible. Coverage includes:

- Hosted servers - Windows, UNIX, Citrix
- Workstation OS – Windows
- Workstation applications - Microsoft Office, Adobe Flash, Adobe Reader and Java
- Hosted databases – MS SQL Server, Oracle
- Cisco network devices

IOT vulnerability management will utilize the following process:

1. Notification and monitoring – IOT will ensure timely notification from reputable sources of vulnerabilities.

2. Assessment – IOT will identify the appropriate course of action to address vulnerabilities. Remediation activities will primarily involve: installation of software patches, adjustment of configuration settings, or removal of affected software. IOT support teams will evaluate the vulnerability and threat level to the environment with an objective of maintaining PCI compliance across state government.

Software patching

Vendor severity ratings, applicability to the state environment, and status of exploits will determine the actions to be taken and timeframes.
Configuration settings

Changes to the configuration may result from a mistake in the initial configuration or as an adjustment to reduce the threat of exploitation by a threat.

Software removal

Removal or uninstalling affected software when it eliminates the vulnerability and associated threats.

Vulnerabilities will be targeted for remediation on the basis of the rating given by IOT’s scanning engine or the vendor affected by the identified vulnerability. On an emergency basis, IOT may take immediate action when a vulnerability exploit poses an imminent threat. Otherwise, vulnerabilities are addressed through a planned, documented, and communicated change control process.

3. Obtainment - IOT will acquire security guidance and software updates only from trusted sources.

4. Testing – IOT will apply patches, apply configuration changes, and eliminate software in test environments established by agencies. Agencies will test appropriately to ensure the updates will not interrupt production systems. Agencies must establish testing groups and promptly notify IOT of problems. If notification is not received it will be assumed the action applied to test environments can be applied to production environments.

5. Deployment – When addressing vulnerabilities classified as “standard” with vendor recommended fix actions, IOT will deploy patches and implement configuration changes on the following schedule:

<table>
<thead>
<tr>
<th>Software</th>
<th>Timeframe</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server OS</td>
<td>within 30 days of release</td>
</tr>
<tr>
<td>Desktop OS</td>
<td>within 90 days of release</td>
</tr>
<tr>
<td>Oracle and SQL Databases</td>
<td>within 90 days of release</td>
</tr>
<tr>
<td>Citrix</td>
<td>within 90 days of release</td>
</tr>
<tr>
<td>Desktop applications</td>
<td>within 90 days of release</td>
</tr>
<tr>
<td>Cisco devices</td>
<td>within 180 days of release</td>
</tr>
</tbody>
</table>

Note: Actions categorized as Emergency and Elevated actions will be handled on a case by case basis but may require more aggressive testing and implementation schedules.

6. Validation – IOT will verify that vulnerability remediation has been executed. The primary tool for this verification will be a vulnerability scanner. The scanner will be used to confirm vulnerability remediation maintains PCI compliance.

Roles

IOT Personnel
Information Asset Owners/System Owners

Responsibilities

Agencies requiring faster or slower vulnerability remediation from IOT can have their needs met through IOT's standard change control process.

Management Commitment

Management that preside over systems/devices shall ensure that scanning and patching occur in accordance with the requirements of this Standard.

Coordination Among Organizational Entities

Agencies shall coordinate with IOT for vulnerability scanning and patching of software.
Compliance
IOT will use a vulnerability scanner confirm latest patching on servers, workstations and other infrastructure related components are in compliance. Agencies are expected to present plans to address the vulnerabilities in a timely manner.

Exceptions
Exceptions will be handled on a case by case basis through the Director of Risk & Compliance and State CISO.