|  |
| --- |
| **Vulnerability Assessment**  **for**    **Jet Black Speed LLC**  **TXARNG DCO-E (Team 21)**                **Version 2**      **May 18, 2018**          **Prepared by**  CPT Rachel Rinaldi  Asst Team Lead  TXARNG DCO-E    **FOR OFFICIAL USE ONLY** |

**Document Revision History**

This Jet Black Speed LLC Vulnerability Assessment Report (VAR) is a living document that is changed as required to reflect system, operational, or organizational changes.  Modifications made to this document are recorded in the version history matrix below.

This document history shall be maintained throughout the life of the document and the associated system.

| **Date** | **Description** | **Version** | **Author** |
| --- | --- | --- | --- |
| 05/18/2018 | Document Publication | 1.0 | Program Office |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Vulnerability Assessment Report Approval Signatures**

I have reviewed the Jet Black Speed LLC Vulnerability Assessment Report and accept the analysis and findings within.

|  |  |
| --- | --- |
|  |  |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_ |
| LTC Jeremy Sereno | Date |
| Security Assessor, TXARNG Team Lead |  |
|  |  |
|  |  |
|  |  |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_ |
| Charles Washington | Date |
| Network Owner, Dir. IT |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

**Table of Contents**

[1 Overview 5](#_Toc514396402)

[2 Network Overview 7](#_Toc514396403)

[2.1 System Name 7](#_Toc514396404)

[2.2 General System Description and Purpose 7](#_Toc514396405)

[2.3 System Characterization 7](#_Toc514396406)

[3 Assessment Methodology 9](#_Toc514396407)

[4 Risk Assessment Results 13](#_Toc514396408)

[4.1 Executive Risk Summary 14](#_Toc514396409)

# Overview

This document represents the *Vulnerability Assessment Report (VAR)* for Jet Black Speed LLC. This VAR contains the results of the comprehensive vulnerability test and evaluation of the Jet Black Speed LLC network. This assessment report, and the results documented herein, supports efforts necessary of a Cyber Incident Response Plan. The VAR describes the risks associated with the vulnerabilities identified during Jet Black Speed LLC’s vulnerability assessment and also serves as the risk summary report as referenced in *NIST SP 800-3 Revision 1, Establishing a Computer Security Incident Response Capability (CSIRC)*.

All assessment results have been analyzed to provide both the network system owner and the authorizing officials with an assessment of the identified vulnerabilities and threats.

**1.1 Applicable Laws and Regulations**

The following laws and regulations are applicable to the Cyber Incident Response Team (TXARNG – DCO-E):

* Computer Fraud and Abuse Act [PL 99-474, 18 USC 1030]
* Freedom of Information Act as Amended in 2016
* Guidance on Inter-Agency Sharing of Personal Data, Protecting Personal Privacy [OMB Memo M-01-05]
* Homeland Security Presidential Directive-7, Critical Infrastructure Identification, Prioritization, and Protection [HSPD-7]
* Homeland Security Presidential Directive-12, Policy for a Common Identification Standard for Federal Employees and Contractors, August 2005
* Implementation of Homeland Security Presidential Directive 12, Policy for a Common Identification
* Management’s Responsibility for Internal Control [OMB Circular A-123, Revised 12/21/2004]
* Privacy Act of 1974 as amended [5 USC 552a]
* Protection of Sensitive Agency Information [OMB M-06-16]
* Records Management by Federal Agencies [44 USC 31]
* Responsibilities for the Maintenance of Records About Individuals by Federal Agencies [OMB Circular A-108, as amended]
* Security of Federal Automated Information Systems [OMB Circular A-130, Appendix III]
* Standing Rules for Use of Cyber (RUC) [Cyber Shield 2018]

**1.2 Applicable Standards and Guidance**

The following standards and guidance are applicable to the organization:

* Computer Security Incident Handling Guide [NIST SP 800—61, Revision 1]
* Contingency Planning Guide for Federal Information Systems [NIST SP 800-34, Revision 1]
* Engineering Principles for Information Technology Security (A Baseline for Achieving Security) [NIST SP 800-27, Revision A]
* Guide for Developing the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach [NIST SP 800-37, Revision 1]
* Guide for Mapping Types of Information and Information Systems to Security Categories [NISP SP 800-60, Revision 1]
* Guide for Security-Focused Configuration Management of Information Systems [NIST SP 800-128]
* Information Security Continuous Monitoring for Federal Information Systems and Organizations [NIST SP 800-137]
* Managing Information Security Risk [NIST SP 800-39]
* Minimum Security Requirements for Federal Information and Information Systems [FIPS Publication 200]
* Risk Management Guide for Information Technology Systems [NIST SP 800-30]
* Security Considerations in the System Development Life Cycle [NIST SP 800-64, Revision 2]
* Technical Guide to Information Security Testing and Assessment [NIST SP 800-115]

**1.3 Purpose**

The Texas Army National Guard Defensive Cyber Operation Element (DCO-E) was activated with the intent to assess, monitor, and mitigate cyber threats in coordination with the Jet Black Speed LLC organization and network owner. The DCO-E has conducted incident response in accordance with the NIST Cyber Security Framework without interruption to Jet Black Speed, LLC. A vulnerability assessment has been performed on Jet Black Speed LLC to evaluate the system’s baseline security controls and evaluate cyber threat potential.

**1.4 Scope**

This VAR applies to Jet Black Speed LLC which has a unique identifier, name, and acronym, noted in Section 2.1.

Documentation used by the assessor to perform the assessment of Jet Black Speed LLC includes the following:

• Jet Black Speed LLC Cyber Security Incident Response Plan

• Jet Black Speed LLC Policies and Code of Conduct

• Jet Black Speed LLC Information Security Policy

• Jet Black Speed LLC & Blue Team 21 Memorandum of Understanding

• Jet Black Speed LLC Remote Access Policy

• Jet Black Speed LLC Server Security Policy

• Jet Black Speed LLC Acceptable Use Policy

• Jet Black Speed LLC Email Policy

Jet Black Speed LLC is physically located at the facilities and location noted below.

| **Site Name** | **Address** |
| --- | --- |
| **Jet Black Speed, LLC** | **Washington, DC**  **Bldg 359** |

# Network Overview

## System Name

| **Unique Identifier (UUID)** | **Information System Name** | **Information System Abbreviation** |
| --- | --- | --- |
| 1 | Jet Black Speed LLC | JBS |

## General System Description and Purpose

Jet Black Speed LLC integrates alternative fuel and energy strategies to power future transportation needs. They currently provide intelligent transportation and tolling solutions. Their network system’s intent is to support the operations of their organization and the transactional processing of their payment system.

## System Characterization

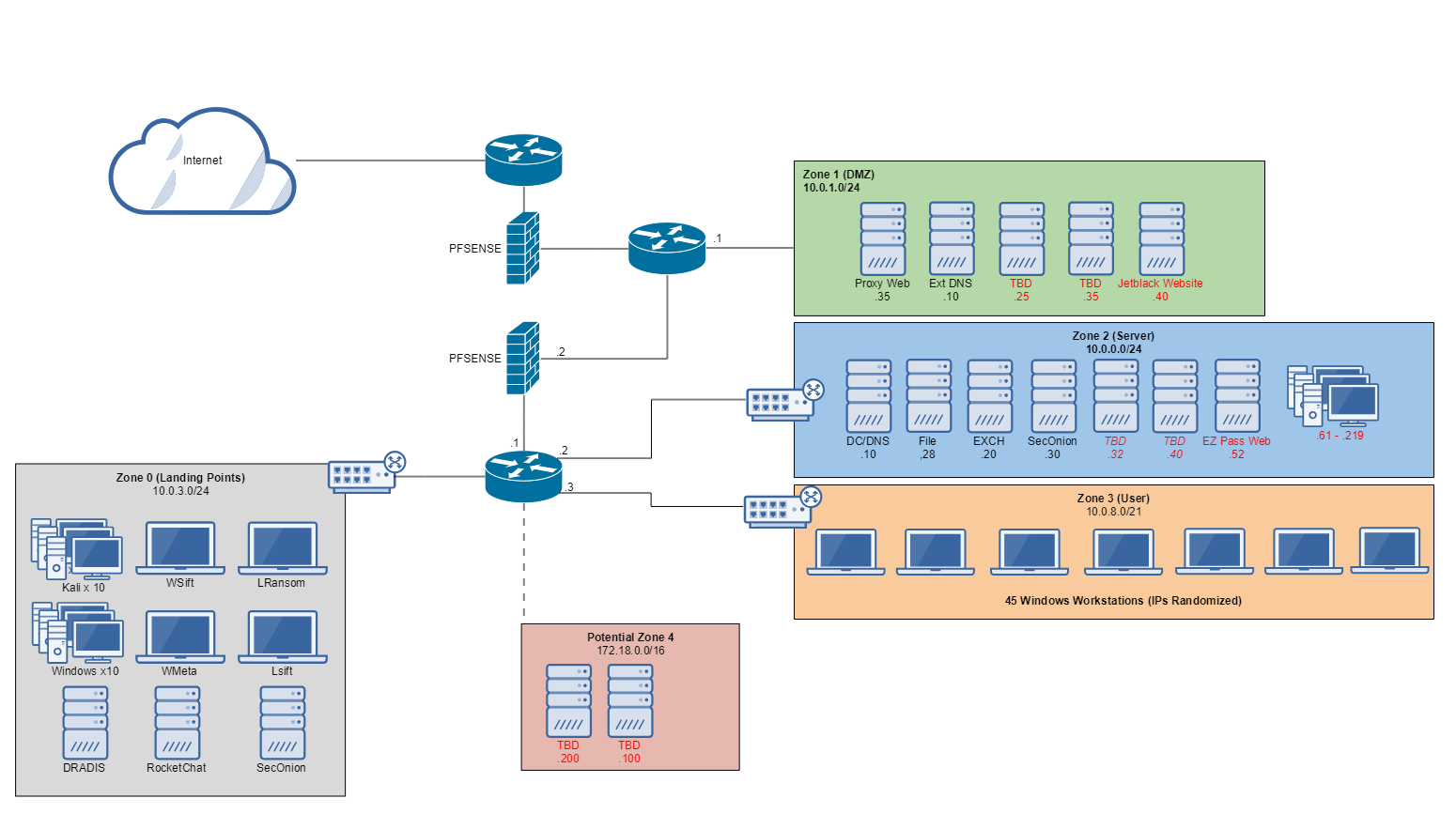
**2.3.1 Technology Components**

| **Component** | **Description** |
| --- | --- |
| Applications | Active Directory, Exchange, MySQL, TomCat and Apache Webserver |
| Operating Systems | Windows 7/Window 10/Ubuntu Linux |
| Networks | Zone 1 (DMZ) - 10.0.1.0/24  Zone 2 (Server) - 10.0.0.0/24  Zone 3 (User) - 10.0.8.0/21 |

**2.3.2 Network Schematic**

The network is established across three zones to support the operations of Jet Black LLC.

| **Zone** | **Critical Infrastructure** |
| --- | --- |
| 1 – DMZ | Proxy Webserver  External DNS  Conference Server  JetBlack LLC Webserver (External) |
| 2 – Server | Domain Controller  Mail Server  File Server  Security Onion (Monitoring)  GrayLog (Logging)  EZ Pay System Webserver |
| 3 – Users | Workstations (48) |

* + 1. **Network Diagram**

**2.3.4 Network Monitoring**

Jet Black LLC’s network consists of a SecurityOnion server responsible for monitoring the network for threats to the system. Upon assessment, the DCO-E discovered the SecurityOnion server was improperly configured and accurate monitoring was not enabled. The DCO-E received approval to reconfigure the SecurityOnion server and execute monitoring activities.

# Assessment Methodology

The security assessment use as logical and prescriptive process for determining risk exposure for the purpose of facilitating decisions as is aligned with the Risk Management Framework (RMF) described in NIST 800-3, Revision 1, *Establishing a Computer Security Incident Response Capability (CSIRC)*. The RMF describes six steps that apply to the system development life-cycle and assessing security controls constitutes Step 4 as illustrated in Figure 4-1.

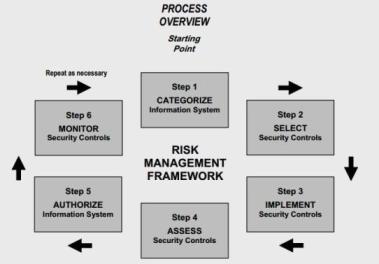


Figure 3-1: Risk Management Framework

This methodology used to conduct the risk assessment for Jet Black Speed LLC system is summarized in the following steps:

1.  Identify vulnerabilities on the platform

2.  Identify threats and determine which threats are associated with the cited vulnerabilities

3.  Analyze risks based on vulnerabilities and associated threats

4.  Recommend corrective actions

5.  Document the results

**3.1 Identification of Vulnerabilities**

A vulnerability is an inherent weakness in an information system that can be exploited by a threat or threat agent, resulting in an undesirable impact in the protection of the confidentiality, integrity, or availability of the system. A vulnerability may be due to a design flaw or error in configuration which makes your network, or a host on your network, susceptible to malicious attacks from local or remote users. Vulnerabilities can exist in multiple areas of your system or facilities, such as in your firewalls, application servers, Web servers, operating systems or fire suppression systems.

Whether or not a vulnerability has the potential to be exploited by a threat depends on a number of variables including (but not limited to):

• The strength of the security controls in place

• The ease at which a human actor could purposefully launch an attack

• The probability of an environmental event or disruption in a given local area

An environmental disruption is usually unique to a geographic location. Depending on the level of the risk exposure, the successful exploitation of a vulnerability can vary from disclosure of information about the host to a complete compromise of the host. Risk exposure to organizational operations can affect the business mission, functions, or the organizational reputation.

The vulnerabilities that were identified through security control testing (including penetration testing) for the Jet Black Speed LLC are identified in *Table 4.1: Risk Assessment Results.*

**3.2 Consideration of Threats**

A threat is an adversial force or phenomenon that could impact the availability, integrity, or confidentiality of an information system and its networks including the facility that houses the hardware and software. A threat agent is an element that provides the delivery mechanism for a threat. An entity that initiates the launch of a threat agent is referred to as a threat actor.

A threat actor might purposefully launch a threat agent (e.g. a terrorist igniting a bomb). However, a threat actor could be a trusted employee that acts as an agent by making an unintentional human error (e.g. a trusted staff clicks on a phishing email that downloads malware). Threat agents may also be environmental in nature with no purposeful intent (e.g. a hurricane). Threat agents working alone, or in concert, exploit vulnerabilities to create incidents. The TXARNG DCO-E categorizes threats using a threat origination taxonomy of P, U, or E type threats as described in Table 3-1.

Table 3-1. Threat Categories and Origination

| **Threat Origination Category** | **Origination Identifier** |
| --- | --- |
| Threats launched purposefully | P |
| Threats created by unintentional human or machine errors | U |
| Threats caused by environmental agents or disruptions | E |

Purposeful threats are launched by threat actors for a variety of reasons and the reasons may never be fully known. Threat actors could be motivated by curiosity, monetary gain, political gain, social activism, revenge or many other driving forces. It is possible that some threats could have more than one threat origination category.

Some threat types are more likely to occur than others. The TXARNG DCO-E takes threat types into consideration to help determine the likelihood that a vulnerability could be exploited. The threat table shown in Table 3-2 is designed to offer typical threats to information systems and these threats have been considered for Jet Black Speed LLC.

Table 3-2. Potential Threats

| **Threat Name** | **Origination Identifier** | **Description** | **Typical Impact to Data or System** | | | **Impact Level** | **Likelihood** | **Risk** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Confidentiality** | **Integrity** | **Availability** |
| DDoS | P | A distributed denial of service (DDoS) is when a malicious user utilizes a zombie network to sabotage a specific website or server. The increased volume of traffic overloads the website or server which causes slow response time or a server to shut down completely |  |  | X | H | H | H |
| Phishing | P/U | A phishing attack is caused by a human sending an email purporting a reputable organization/activity in order to induce an individual to reveal personal information such as passwords, PII, or PCI. | X | X |  | M | H | M |
| RansomWare | P | Malicious software that threatens to publish the victim’s data or perpetually block access to a system unless a random is paid. | X | X | X | H | M | M |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |

**3.3 Perform Risk Analysis**

The goal of determining risk exposure is to facilitate decision making on how to respond to real and perceived risks. The outcome of performing a risk analysis, yields risk exposure metrics that can be used to make risk-based decisions.

The TXARNG DCO-E risk analysis process is based on qualitative risk analysis. In qualitative risk analysis the impact of exploiting a threat is measured in relative terms. When a system is easy to exploit, it has a High likelihood that a threat could exploit the vulnerability. Likelihood definitions for the exploitation of vulnerabilities are found in Table 3-3.

Table 3-3. Likelihood Definitions

| **Likelihood** | **Description** |
| --- | --- |
| Low | There is little to no chance that a threat could exploit a vulnerability and cause loss to the system or its data. |
| Moderate | There is a moderate chance that a threat could exploit a vulnerability and cause loss to the system or its data. |
| High | There is a high chance that a threat could exploit a vulnerability and cause loss to the system or its data. |

Impact refers to the magnitude of potential harm that could be caused to the system (or its data) by successful exploitation. Definitions for the impact resulting from the exploitation of a vulnerability are described in Table 3-4. Since exploitation has not yet occurred, these values are perceived values. If the exploitation of a vulnerability can cause significant loss to a system (or its data) then the impact of the exploit is considered to be High.

Table 3-4. Impact Definitions

| **Impact** | **Description** |
| --- | --- |
| Low | If vulnerabilities are exploited by threats, little to no loss to the system, networks, or data would occur. |
| Moderate | If vulnerabilities are exploited by threats, moderate loss to the system, networks, and data would occur. |
| High | If vulnerabilities are exploited by threats, significant loss to the system, networks, and data would occur. |

The combination of High likelihood and High impact creates the highest risk exposure. The risk exposure matrix shown in Table 3-5 presents the same likelihood and impact severity ratings as those found in *NIST SP 800-30 Risk Management Guide for Information Technology Systems.*

Table 3-5. Risk Exposure Ratings

| **Likelihood** | **Impact** | | |
| --- | --- | --- | --- |
| **Low** | **Moderate** | **High** |
| High | Low | Moderate | High |
| Moderate | Low | Moderate | Moderate |
| Low | Low | Low | Low |

**3.4 Document Results**

Documenting the results of security testing creates a record of the security posture for the system at a given moment in time. The record can be reviewed for risk-based decision making and to create plans of action to mitigate risks.

# Risk Assessment Results

This section describes all security weaknesses found during testing. The following elements for each security weakness are reported:

* Finding Number
* Status
* Source
* Risk
* Business Impact Statement
* Recommended Corrective Action
* Link to Control(s)/Test Case(s)
* Likelihood
* Impact
* Risk Level

The reader of the VAR should anticipate that the security weakness elements are described as indicated below.

* **Finding Number:** The unique application-generated security finding number.
* **Status:** The computed lifecycle status associated with the finding.  If the finding is linked to a weakness for remediation management, the finding status is computed based on the completed status of the weakness.  Finding status described below:
  + **Unlinked** - The finding is not linked to a weakness.
  + **Active** - The finding has been linked to a weakness that has an open status.
  + **Completed** - The finding has been linked to a weakness where remediation has been completed successfully (i.e. the weakness is in completed status).
  + **Rejected** - The finding has been rejected either as a false positive or risk accepted (i.e. risk-based decision).  No remediation is required for the security finding.
* **Source:**The finding type such as vulnerability assessment, security audit, etc., and the failed security control in which the finding was created.
* **Risk:** The finding description.  This is the description of the finding as defined from the vulnerability assessment, security audit report, or from the results of an internal security review.
* **Business Impact Statement:** Impact of the finding to the organization if exploited.
* **Recommended Corrective Action:** The recommended control(s) needed to remediate the finding.
* **Link to Control(s)/Test Case(s):** The control and/or test case associated with the finding.
* **Likelihood:** The likelihood that the finding will be exploited (High, Moderate, or Low).
* **Impact:**The impact to the organization if the finding is exploited (High, Moderate, or Low).
* **Risk Level:** The computed risk level associated with the finding based on the selected likelihood and impact.  Please refer to Table 3-5 Risk Exposure Ratings for details.

## Executive Risk Summary

This section provides a high-level summary of the most pertitnent risks/vulernabilities discovered within the Jet Black Speed LLC system.

**Protective Systems:** Numerous vulnerabilities were discovered pertaining to the protective systems of the network.

* No antivirus software was running for any host across Zone 1, 2, or 3.
* The PFSense Firewall components were not configured properly and allowing all inbound and outbound traffic throughout the network.
* The SecurityOnion monitoring tool was not configured or properly executing.

**Network Traffic & User Control:** The assessment discovered numerous flaws within the connectivity and traffic control throughout all zones within the network.

* Unnecessary ports, services and protocols were enabled
* Unauthorized users were allowed elevated privileges and default passwords within the hosts and users were utilized
* Phishing attempts were successful due to users

**Network Containment:** The assessment discovered an additional unidentified network in the system

* An unidentified network was discovered which potential to allow unauthorized inbound and/or outbound traffic

**Table 4-1. Vulnerability Assessment Results**

| **ID** | **Network Zone** | **Vulnerability** | **Remediation Actions** | **Risk Level** |
| --- | --- | --- | --- | --- |
| **1** | All | Antivirus is not installed | Install an antivirus on all hosts and clients to protect against threats | **H** |
| **2** | All | Default passwords through out network assets | Modify default passwords for assets to better secure the network from unauthorized access | **H** |
| **3** | All | Elevated privileges of user accounts | Users with elevated privileges could execute unauthorized actions on the network | **H** |
| **4** | All | Open and unnecessary ports across the network | Close unnecessary ports throughout the network | **H** |
| **5** | All | Unnecessary and legacy services active within the network | Disable useless  services, Monitor service used by users. | **H** |
| **6** | 2 | Spank.c -- your machine answers to TCP packets that are coming from a multicast address -- attackers might use this flaw to shutdown this server and saturate your network; can also be used to run stealth scans against your machine | Contact your OS vendor for a patch and filter out multicast addresses (224.0.0.0/4) | **M** |
| **7** | 2 | SSL/TLS: Report Weak Cipher Suites | Recommended to disable weak Ciphers and SSL 2.0 and 3.0 in Apache | **M** |
| **8** | 2 | SSL/TLS: Certificate using weak signature algorithm | Servers using SHA-1 signatures will need to obtain new SHA-2 signed SSL/TLS certificates | **M** |
| **9** | 2 | DH Key Exchange Insufficient Group Strength. Cipher susceptible to log jam attack. Effect to Websites, mail servier, and other TLS dependent services | Web or Mail server.  Disable support for export cipher suites using 2048-bit DH group. Update to recent version of OpenSSH. Browser= Updates most recent version and check for updates | **M** |
| **10** | 2 | OpenSSL Death Alert DoS. Remote user can consume excessive CPU resources on the target system. | Openssl.org issued fix. | **M** |
| **11** | 2 | RC4 Algorithm, Used in TLS and SSL protocol. Allows unauthorized disclosure of information | Support TLS 1.2 and GCM suites. Disable TLS compression. Monitor products likely use the protoc | **M** |
| **12** | 2 | Apache Tomcat with HTTP PUTs enabled. | Remove default files, ex: JSP’s and servlets from the Tomcat Servlet/JSP container | **M** |
| **13** | 2 | MS Windows SMTP Server DNS Spoofing. MIM attackers can  spoof DNS responses. MS Exchange if affected by these vulnerabilities. | Microsoft Fixed these vulnerabilities as part of MS 10-024 | **M** |
| **14** | 2 | Header Overflow against HTTP proxy | Upgrade your software | **M** |

| **ID** | **Network Zone** | **Vulnerability** | **Remediation Actions** | **Risk Level** |
| --- | --- | --- | --- | --- |
| **15** | 2/3 | Remote Code Execution Vulnerability | Apply recommended Windows Hotfix (MS15-034) | **M** |
| **16** | 2 | Mongoose Web Server Remote Buffer Overflow. Allows remote attackers to execute arbitrary code via an HTTP PUT request.DOS | OpenWall.com found fix. Add line in source code to avoid a buffer overflow. | **M** |
| **17** | 2 | Apache Struts Dynamic Method Invocation Remote Code Execution -- allows unauthorized modification and disruption of service | Vendor Recommendation:  Disable Dynamic Method Invocation when possible or upgrade to Apache Struts versions 2.3.20.3, 2.3.24.3 or 2.3.28.1. | **H** |
| **18** | All | IPV6 | LLMNR (Link-Local Multicast Name Resolution) | DHCP | Do not utilize IPv6 | **M** |
| **19** | 2 | SMTP Server on anomalous Ports | Clean configuration to use standard SMTP ports. | **L** |
| **20** | 3 | Non-standard share on client with everyone permissions can allow files to be moved without corporate knowledge | Disable share access upon start-up | **M** |
| **21** | All | SMB enabled on all hosts | Disable SMB1 | **M** |
|  | 3 | Phishing scam from suspected malicious IP | Implement Phishing scam training and policies | **M** |
|  |  |  |  |  |