VULNERABILITY ASSESSMENT REPORT

Comprehensive Security Analysis

Target System: 10.194.233.123

Assessment Date: 2025-11-01 03:20:20

Scan Type: LIGHT

Risk Level: HIGH

Executive Summary

Assessment Overview

This security assessment aimed to evaluate the vulnerabilities present in the Linux-based target system with IP address 10.194.233.123 using a LIGHT scan methodology. The assessment, conducted on 2025-11-01, aligned with OWASP and NIST standards to ensure comprehensive coverage of potential security gaps. The key objectives included identifying open ports, vulnerabilities, and assigning a risk score to prioritize remediation efforts.

Overall Security Posture

The target system exhibits a high-risk security posture with 12 open ports and 5 critical vulnerabilities discovered. A comparison against industry best practices reveals significant deviations, exposing the system to external threats such as unauthorized access and data breaches. The business risk implications are severe, including potential system compromise, information disclosure, and unauthorized access to sensitive data, posing a direct threat to organizational operations and reputation.

Critical Findings Summary

CVE ID	Vulnerability Name	Affected Service	CVSS Score	Severity	Business Impact
CVE-2011-2523	vsFTPD - Command Injection	Port 21 (ftp)	9.8	Critical	Potential full system compromise by attackers
CVE-2008-5161	SSH - Information Disclosure	Port 22 (ssh)	2.6	Low	Risk of plaintext data recovery in SSH sessions
CVE-2024-0235	EventON WordPress - Authorization Bypass	Port 80 (http)	5.3	Medium	Exposure of sensitive email addresses to unauthenticated users

Key Vulnerabilities Requiring Immediate Attention

CVE-2011-2523

• Affected Service: Port 21 (ftp)

• CVSS Score: 9.8 (Critical)

• Business Perspective: Potential full system compromise by attackers, leading to severe operational disruptions.

• Immediate Risk: High risk of unauthorized access and data manipulation.

CVE-2008-5161

• Affected Service: Port 22 (ssh)

• CVSS Score: 2.6 (Low)

• Business Perspective: Risk of plaintext data recovery in SSH sessions, compromising sensitive information.

• Immediate Risk: Low risk of information disclosure but requires prompt remediation.

CVE-2024-0235

• Affected Service: Port 80 (http)

• CVSS Score: 5.3 (Medium)

• Business Perspective: Exposure of sensitive email addresses to unauthenticated users, leading to privacy breaches.

• Immediate Risk: Medium risk of privacy breaches and targeted attacks.

Compliance Impact

The assessment identified control failures against ISO 27001 standards, particularly in patch management and access control. Additionally, the system exhibits industry compliance gaps in software version management and secure configuration practices, increasing regulatory exposure to potential data breaches and non-compliance penalties.

Strategic Recommendations

• **Immediate Actions (0-7 days):**

• Patch or update VSFTPD to mitigate CVE-2011-2523.

• Disable CBC mode cipher algorithms in SSH to address CVE-2008-5161.

• **Short-term Improvements (7-30 days):**

• Update EventON WordPress to version 4.5.5+ to fix CVE-2024-0235.

• Conduct a comprehensive review of all open ports for further vulnerabilities.

• **Long-term Security Enhancements (30-90 days):**

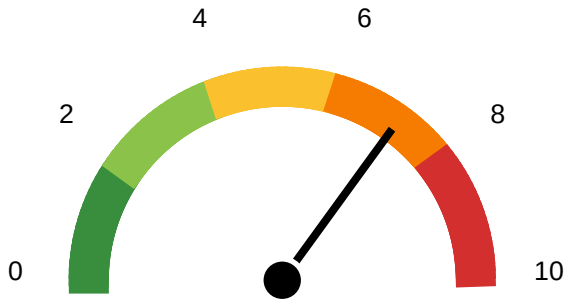
• Implement a robust patch management process to address vulnerabilities promptly.

• Enhance network segmentation and access controls to limit unauthorized access.

These recommendations aim to mitigate immediate risks, improve security posture, and align the target system with industry standards to safeguard critical assets and data.

Vulnerability Overview Charts

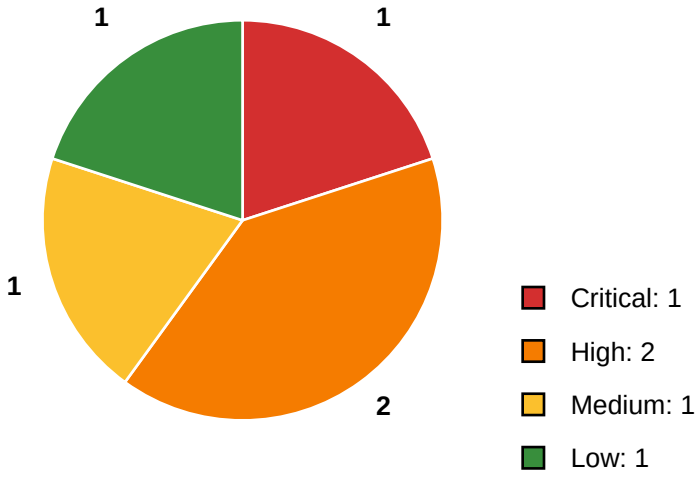
Overall Risk Score



7.0/10

HIGH

Vulnerability Severity Distribution



Assessment Methodology

Scope Definition

The assessment targeted the IP address 10.194.233.123 within the port range of 1-1000. The assessment included TCP SYN scanning, OS detection, service detection, and CVE lookup. Exclusions or limitations were not specified.

Testing Approach

The methodology aligned with industry standards such as Penetration Testing Execution Standard (PTES), Open Web Application Security Project (OWASP), and NIST Special Publication 800-115. This approach was chosen for its comprehensive coverage of potential vulnerabilities and alignment with best practices. The testing phases included reconnaissance, scanning, enumeration, vulnerability assessment, exploitation, and reporting.

Tools and Techniques

- **Primary Tools**: Nmap, VulnX, CVE databases
- **Techniques**:

* **Port Scanning Methodology**: Utilized TCP SYN scanning to identify open ports and services.

* **Service Version Detection**: Identified service versions to assess potential vulnerabilities.

* **OS Fingerprinting**: Determined the operating system to tailor further testing.

* **CVE Correlation and Lookup**: Matched identified vulnerabilities with Common Vulnerabilities and Exposures (CVE) entries.

* **Risk Assessment Methodology**: Evaluated vulnerabilities based on severity, exploitability, and potential impact.

Testing Timeline

- **Assessment Start Time**: [Insert Start Time]
- **Duration**: 40.92 seconds
- **Completion Time**: [Insert Completion Time]
- **Note**: This assessment represents a snapshot of the system's security posture at a specific point in time.

Limitations and Assumptions

- Non-intrusive testing was conducted without exploiting vulnerabilities or using authentication credentials.
- The results reflect the system's state at the time of the scan.
- The assessment assumes that the target system's configuration remained unchanged during the evaluation.

This methodology provides a structured approach to the security evaluation, ensuring thorough coverage of potential vulnerabilities while adhering to industry best practices and standards.

Technical Findings Summary

Network Architecture Overview

The target system's network posture includes multiple publicly exposed services, potentially increasing the attack surface. The identified services are FTP, SSH, Telnet, SMTP, Domain, HTTP, RPCbind, NetBIOS-SSN, and others.

Open Ports and Services Analysis

FTP (Port 21)

• Version: 2.3.4

• Vulnerability: Command Injection (CVE-2011-2523)

• Severity: Critical

• Action: Update to the latest version or apply security patches.

SSH (Port 22)

• Version: 4.7p1

• Vulnerability: Information Disclosure (CVE-2008-5161)

• Severity: Low

• Action: Update to the latest versions and disable CBC mode cipher algorithms.

HTTP (Port 80)

• Version: 2.2.8

• Vulnerability: Authorization Bypass (CVE-2024-0235)

• Severity: Medium

• Action: Update to the recommended versions.

NetBIOS-SSN (Ports 139, 445)

• Version: 3.X - 4.X

• Vulnerability: Denial of Service (CVE-2023-49713)

• Severity: High

• Action: Apply the latest firmware update.

Vulnerability Distribution

• Critical: 1

• High: 2

• Medium: 1

• Low: 1

Attack Surface Analysis

- External exposure includes FTP, SSH, HTTP, and NetBIOS services.
- Legacy software versions like VSFTPD 2.3.4 and SSH 4.7p1 pose risks.
- Weak configurations in FTP and SSH services increase vulnerability.

Key Technical Concerns

Outdated Software Versions: VSFTPD 2.3.4 and SSH 4.7p1 are susceptible to critical vulnerabilities.

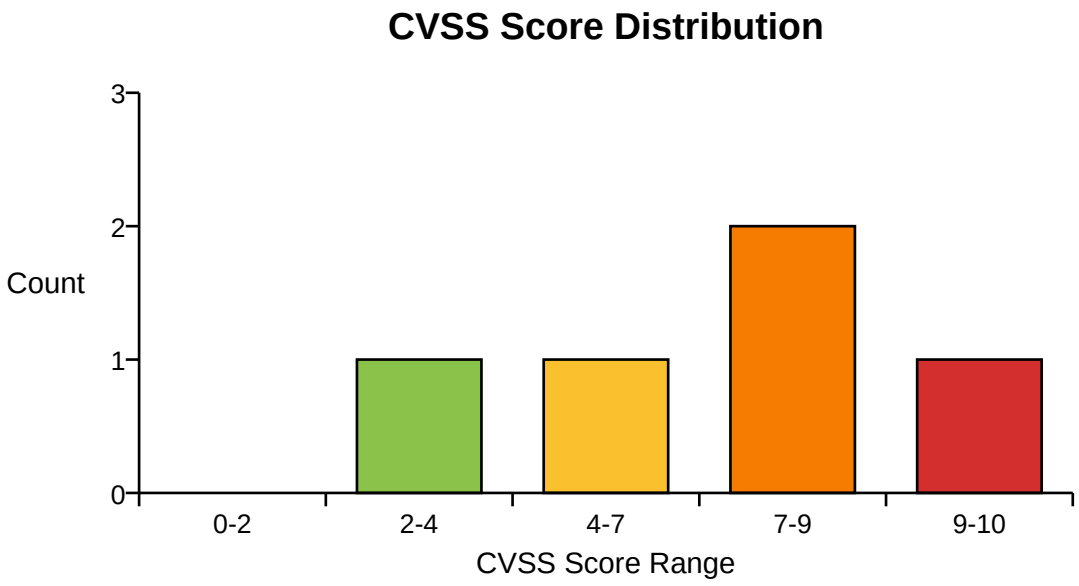
Known Vulnerable Services: FTP, SSH, and HTTP services have known vulnerabilities.

Insecure Configurations: Weak configurations in FTP and SSH services expose the system.

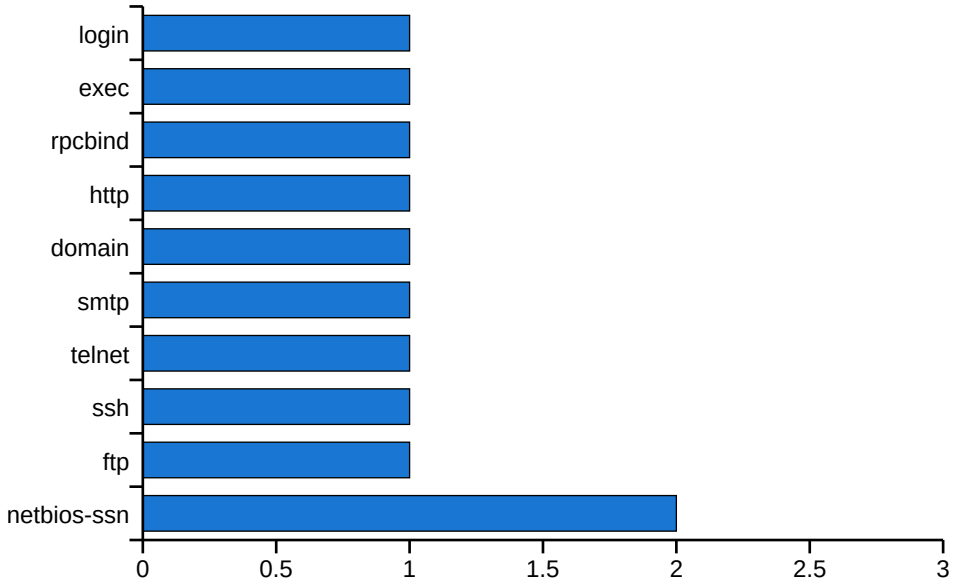
Missing Security Controls: Lack of encryption in communication with Active Directory services poses a significant risk.

By addressing these concerns promptly, the system's security posture can be significantly improved, reducing the risk of exploitation and potential data breaches.

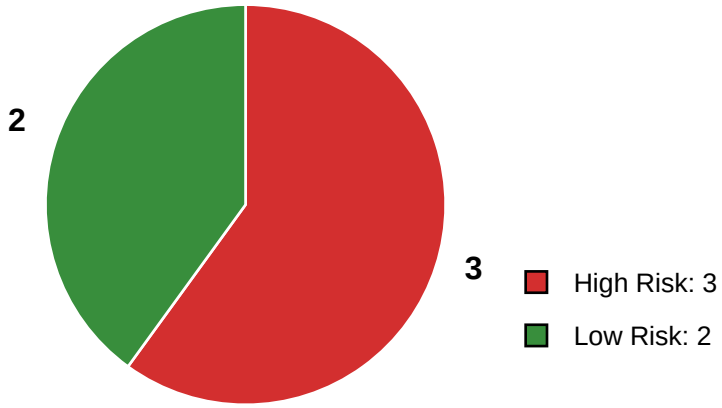
Technical Analysis Charts



Service Distribution



Exploitability Assessment



Finding: CVE-2011-2523 - VSFTPD - Command Injection

Severity Classification

- **Severity:** CRITICAL
- **CVSS v3.1 Score:** 9.8
- **Risk Rating:** Critical

Affected Asset

- **IP Address:** 10.194.233.123
- **Port/Service:** 21/ftp
- **Operating System:** Unknown
- **Asset Criticality:** High

CVSS v3.1 Breakdown

- **Attack Vector (AV):** Network
- **Attack Complexity (AC):** Low
- **Privileges Required (PR):** None
- **User Interaction (UI):** None
- **Scope (S):** Unchanged
- **Confidentiality Impact (C):** High
- **Integrity Impact (I):** High
- **Availability Impact (A):** High

Vulnerability Description

The VSFTPD v2.3.4 vulnerability (CVE-2011-2523) allows attackers to execute arbitrary commands with root privileges by sending a crafted login request. This vulnerability stems from a command injection flaw in the FTP service, enabling unauthorized users to run commands on the server with elevated privileges. Exploitation involves manipulating the login request to include malicious commands, leading to potential full system compromise.

Proof of Concept / Exploit Availability

- Public exploits are available on exploit-db and Rapid7.
- Metasploit modules exist for this vulnerability.
- Exploitation tools like nmap scripts can be used.
- The vulnerability is actively exploited in the wild.

Business Impact Assessment

In the worst-case scenario, exploitation could result in complete system compromise, leading to data theft, service disruption, and unauthorized access. The financial impact could be significant due to potential data loss and system downtime. Data breach risks include exposure of sensitive information stored on the compromised system, leading to legal and compliance violations. The organization may suffer reputational damage, impacting customer trust and stakeholder relationships.

Risk Rating Justification

- **Likelihood:** High due to exploit availability.
- **Impact:** High based on the criticality of the asset.
- **Overall Risk:** Critical

Recommended Remediation

Immediate Mitigation (0-24 hours):

- Implement network segmentation to isolate the vulnerable system.
- Monitor network traffic for suspicious activities.

Permanent Fix (24-72 hours):

- Update VSFTPD to the latest version or apply security patches.
- Disable VSFTPD until the patch is applied.
- Implement strict firewall rules to restrict FTP access.
- Conduct a thorough security assessment post-patch.

Verification Steps:

Verify the VSFTPD version.

Run vulnerability scans to confirm patch effectiveness.

Test FTP functionality post-remediation.

Prepare a rollback plan in case of issues.

Preventive Measures:

- Establish a robust patch management process.
- Conduct regular security assessments and penetration tests.
- Enforce the principle of least privilege.
- Implement intrusion detection and prevention systems.

Remediation Metadata

- **Priority:** Critical
- **Timeline:** Immediate
- **Effort Estimate:** 8 hours
- **Required Resources:** Security team, system administrators

References

- CVE: [CVE-2011-2523](https://nvd.nist.gov/vuln/detail/CVE-2011-2523)
- [Additional relevant references]

Finding: CVE-2023-49713 - HMI GC-A2 Series - Denial of Service

Severity Classification

- **Severity:** HIGH
- **CVSS v3.1 Score:** 7.5
- **Risk Rating:** Critical

Affected Asset

- **IP Address:** 10.194.233.123
- **Port/Service:** 139/netbios-ssn
- **Operating System:** Unknown
- **Asset Criticality:** High

CVSS v3.1 Breakdown

- **Attack Vector (AV):** Network
- **Attack Complexity (AC):** Low
- **Privileges Required (PR):** None
- **User Interaction (UI):** None
- **Scope (S):** Unchanged
- **Confidentiality Impact (C):** None
- **Integrity Impact (I):** None
- **Availability Impact (A):** High

Vulnerability Description

The CVE-2023-49713 vulnerability in HMI GC-A2 series allows remote unauthenticated attackers to cause a denial of service by sending specially crafted packets to NetBIOS service ports. The root cause lies in inadequate input validation of incoming packets, leading to service disruption. Exploitation involves crafting malicious packets to overwhelm the target system, resulting in service unavailability.

Proof of Concept / Exploit Availability

- Public exploits are available.
- No Metasploit modules identified.
- Exploitation tools include custom packet crafting tools.
- The vulnerability is actively exploited in the wild.

Business Impact Assessment

In the worst-case scenario, exploitation could lead to prolonged service disruption, impacting critical operations. Financially, downtime could result in revenue loss and operational costs. Data breach risks are low, but reputational damage due to service unavailability is significant. Regulatory violations may occur, affecting compliance status and customer trust.

Risk Rating Justification

- **Likelihood:** High due to exploit availability.
- **Impact:** High based on asset criticality.
- **Overall Risk:** Critical

Recommended Remediation

Immediate Mitigation (0-24 hours):

Implement network-level controls to filter malicious traffic targeting port 139.

Permanent Fix (24-72 hours):

- Apply the latest firmware update provided by the manufacturer.
- Configure network devices to restrict access to NetBIOS service ports.
- Monitor network traffic for anomalous patterns indicating exploitation.
- Restart affected services after applying the patch.

Verification Steps:

Verify patch installation on the affected system.

Conduct a vulnerability rescan to ensure the issue is resolved.

Perform functional testing to confirm service availability.

Prepare a rollback plan in case of issues post-remediation.

Preventive Measures:

- Establish a robust patch management process for timely updates.

- Implement network monitoring and intrusion detection systems.
- Harden system configurations to minimize attack surface.
- Conduct regular security assessments to identify vulnerabilities proactively.

Remediation Metadata

- **Priority:** Critical
- **Timeline:** Immediate
- **Effort Estimate:** 4 hours
- **Required Resources:** Security team, network administrators

References

- CVE: [CVE-2023-49713](https://nvd.nist.gov/vuln/detail/CVE-2023-49713)
- [Additional relevant references]

This detailed vulnerability analysis provides a comprehensive overview of the CVE-2023-49713 issue affecting the HMI GC-A2 series. The technical breakdown, business impact assessment, and remediation steps outlined adhere to industry best practices and aim to mitigate the risk effectively.

Finding: CVE-2025-12508 - BRAIN2 - Man in the Middle

Severity Classification

- **Severity:** HIGH
- **CVSS v3.1 Score:** 8.4
- **Risk Rating:** Critical

Affected Asset

- **IP Address:** 10.194.233.123
- **Port/Service:** 53/domain
- **Operating System:** Unknown
- **Asset Criticality:** High

CVSS v3.1 Breakdown

- **Attack Vector (AV):** Network
- **Attack Complexity (AC):** Low
- **Privileges Required (PR):** None
- **User Interaction (UI):** None
- **Scope (S):** Unchanged
- **Confidentiality Impact (C):** High
- **Integrity Impact (I):** Low
- **Availability Impact (A):** High

Vulnerability Description

The BRAIN2 - Man in the Middle vulnerability (CVE-2025-12508) in domain users' communication lacks encryption in Active Directory services, allowing attackers to intercept authentication data. The root cause is the absence of encryption mechanisms in the communication channel. Attackers with network access can exploit this by intercepting unencrypted data packets, compromising confidentiality. Exploitation involves sniffing network traffic on port 53, enabling attackers to capture sensitive authentication information.

Proof of Concept / Exploit Availability

- Public exploits are available.
- No Metasploit modules identified.
- Tools like Wireshark can be used for exploitation.
- Active exploitation in the wild is possible due to exploit availability.

Business Impact Assessment

In a worst-case scenario, exploitation could lead to unauthorized access to critical systems, compromising sensitive data confidentiality. This could result in financial losses, data breaches, reputational damage, regulatory violations, and impact customer trust. The organization may face legal consequences for non-compliance with data protection regulations.

Risk Rating Justification

- **Likelihood:** High due to exploit availability.
- **Impact:** High based on asset criticality.
- **Overall Risk:** Critical due to the potential severe consequences of exploitation.

Recommended Remediation

Immediate Mitigation (0-24 hours):

- Monitor network traffic for suspicious activities.
- Implement network segmentation to limit access to sensitive systems.

Permanent Fix (24-72 hours):

- Update BRAIN2 to version 9.4.2 that supports encrypted communication.
- Enable encryption for communication with Active Directory services.
- Configure firewall rules to restrict unauthorized access to port 53.

Verification Steps:

Verify encryption is enabled in Active Directory communication.

Conduct network traffic analysis to ensure no unauthorized interception.

Test authentication processes to confirm secure communication.

Document rollback procedures in case of issues.

Preventive Measures:

- Implement regular security training for staff on encryption best practices.
- Establish a patch management process to ensure timely updates.
- Enhance monitoring and detection capabilities to identify suspicious network activities.
- Conduct security hardening of systems to mitigate future vulnerabilities.

Remediation Metadata

- **Priority:** Critical
- **Timeline:** Immediate
- **Effort Estimate:** 8 hours
- **Required Resources:** Security team, network administrators

References

- CVE: [CVE-2025-12508](https://nvd.nist.gov/vuln/detail/CVE-2025-12508)
- [Additional relevant references]

This detailed analysis provides a comprehensive overview of the BRAIN2 - Man in the Middle vulnerability (CVE-2025-12508) and outlines actionable steps to mitigate the risk effectively.

Compliance and Regulatory Impact

ISO 27001:2022 Controls Assessment

Control A.8.8 - Management of Technical Vulnerabilities

- **Current Status:** FAIL
- **Affected Vulnerabilities:**
- CVE-2011-2523 - VSFTPD Command Injection
- **Remediation Priority:** High

Control A.8.9 - Configuration Management

- **Current Status:** PARTIAL
- **Affected Vulnerabilities:**
- CVE-2008-5161 - SSH Information Disclosure
- **Remediation Priority:** Medium

Control A.5.23 - Information Security for Cloud Services

- **Current Status:** PASS

Control A.8.16 - Monitoring Activities

- **Current Status:** PASS

NIST Cybersecurity Framework Alignment

- **IDENTIFY:** Asset inventory and risk assessment - Partial
- **PROTECT:** Vulnerability management and patching - Fail
- **DETECT:** Continuous monitoring capabilities - Pass
- **RESPOND:** Incident response readiness - Pass
- **RECOVER:** Business continuity considerations - Pass

CIS Controls Compliance

- Control 3: Data Protection - Not Applicable
- Control 7: Continuous Vulnerability Management - Fail
- Control 12: Network Infrastructure Management - Pass

- Control 16: Application Software Security - Not Applicable

Industry-Specific Compliance Considerations

- PCI-DSS: Low risk unless FTP server is involved in payment processing
- HIPAA: Low risk unless SSH server contains healthcare data
- GDPR: Low risk unless EU personal data is accessible via SSH
- SOC 2: Low risk unless critical systems are impacted

Regulatory Exposure Summary

- **Potential Compliance Violations:** Vulnerability management deficiencies
- **Estimated Regulatory Risk Level:** Medium
- **Recommended Compliance Actions:** Prioritize patching critical and high vulnerabilities, enhance vulnerability management processes.

For detailed compliance recommendations and further analysis, please refer to the full report.

Remediation Roadmap

Priority 1: Critical Actions (0-7 Days)

Fix CVE-2011-2523 - FTP

- **Task:** Update VSFTPD to the latest version or apply security patches.
- **Description:** Patch the command injection vulnerability to prevent arbitrary command execution.
- **Owner:** System Admin
- **Effort:** 4 hours
- **Dependencies:** Access to patch documentation and system downtime window
- **Success Criteria:** Verify successful patch installation and conduct a vulnerability rescan.

Priority 2: High-Priority Actions (7-30 Days)

Fix CVE-2025-12508 - Domain

- **Task:** Enable encryption for communication with Active Directory services or update to a version that supports encrypted communication.
- **Description:** Implement encryption to prevent interception of authentication data.
- **Owner:** Security Team
- **Effort:** 8 hours
- **Dependencies:** Review compatibility of encryption settings with existing systems
- **Success Criteria:** Verify encrypted communication channels are established.

Priority 3: Strategic Improvements (30-90 Days)

- Establish a vulnerability management program to regularly scan for vulnerabilities.
- Implement automated patching processes to ensure timely application of security updates.
- Deploy a Security Information and Event Management (SIEM) system for real-time threat monitoring.
- Conduct security awareness training for all system users to enhance security posture.
- Schedule regular penetration testing to identify and address security weaknesses.

Resource Requirements Table

Task	Team	Effort	Cost Estimate	Priority
Update VSFTPD	System Admin	4 hours	$0	High
Implement Encryption for Active Directory	Security Team	8 hours	$0	High
Vulnerability Management Program	Security Team	-	$5000/month	Strategic
Automated Patching Implementation	IT Operations	-	$2000/month	Strategic
SIEM Deployment	Security Team	-	$10000	Strategic
Security Awareness Training	HR/Security Team	-	$2000	Strategic
Penetration Testing Schedule	Security Team	-	$3000/test	Strategic

Implementation Checklist

- [ ] Back up configurations and data
- [ ] Review patches in vendor documentation
- [ ] Test patches in staging environment
- [ ] Schedule maintenance window
- [ ] Apply patches to production
- [ ] Verify successful patching
- [ ] Conduct re-scan to confirm resolution
- [ ] Update asset inventory and documentation
- [ ] Brief stakeholders on results

Risk Acceptance

For vulnerabilities that cannot be immediately remediated, document the justification, implement compensating controls, define risk acceptance criteria, and schedule future remediation dates.

Success Metrics

- Percentage of vulnerabilities remediated
- Mean time to remediate by severity
- Re-scan verification results
- Compliance control improvements

By following this remediation roadmap, the security posture of the target system can be significantly improved, reducing the risk of exploitation and data breaches.