VULNERABILITY ASSESSMENT REPORT

Comprehensive Security Analysis

Target System: 10.0.2.9

Assessment Date: 2025-09-30 11:49:17

Scan Type: LIGHT

Risk Level: HIGH

Executive Summary

Assessment Overview

This vulnerability assessment aimed to evaluate the security posture of the Linux system with IP address 10.0.2.9 using a LIGHT scan methodology. The assessment, aligned with OWASP and NIST standards, identified 5 vulnerabilities across 12 open ports, resulting in a high-risk level score of 7.2/10. Key objectives included identifying critical security gaps and providing actionable recommendations for remediation.

Overall Security Posture

The target system exhibits significant vulnerabilities, with 5 critical issues identified, including command injection in VSFTPD, information disclosure in SSH, and an authorization bypass in EventON WordPress. These findings indicate a concerning lack of adherence to industry best practices, exposing the system to external threats such as unauthorized access and data breaches. The high-risk level poses severe business implications, including potential system compromise, information leakage, and reputational damage.

Critical Findings Summary

CVE ID	Vulnerability Name	Affected Service	CVSS Score	Severity	Business Impact	Immediate
CVE-2011-2523	VSFTPD - Command Injection	ftp (Port 21)	9.8	Critical	Arbitrary command execution with root privileges	Full system compron
CVE-2008-5161	SSH - Information Disclosure	ssh (Port 22)	2.6	Low	Plaintext data recovery from SSH sessions	Information disclosur
CVE-2024-0235	EventON WordPress - Auth Bypass	http (Port 80)	5.3	Medium	Unauthenticated access to sensitive email addresses	Privacy breaches

Key Vulnerabilities Requiring Immediate Attention

CVE-2011-2523 (VSFTPD - Command Injection)

• Affected Service: ftp (Port 21)

• CVSS Score: 9.8 (Critical)

• Business Impact: Allows arbitrary command execution with root privileges, leading to full system compromise.

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

CVE-2008-5161 (SSH - Information Disclosure)

• Affected Service: ssh (Port 22)

• CVSS Score: 2.6 (Low)

• Business Impact: Enables plaintext data recovery from SSH sessions, potentially exposing sensitive information.

• Immediate Risk: Low risk of information disclosure.

CVE-2024-0235 (EventON WordPress - Auth Bypass)

• Affected Service: http (Port 80)

• CVSS Score: 5.3 (Medium)

• Business Impact: Allows unauthenticated users to access email addresses, risking privacy breaches.

• Immediate Risk: Medium risk of unauthorized data access.

Compliance Impact

The assessment revealed failures in ISO 27001 controls, particularly in access control and vulnerability management. Additionally, compliance gaps were identified in industry standards, potentially exposing the organization to regulatory penalties and legal consequences.

Strategic Recommendations

• **Immediate Actions (0-7 days):**

• Patch VSFTPD and SSH vulnerabilities to prevent unauthorized access.

• Update EventON WordPress to mitigate the authorization bypass issue.

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

• Implement network segmentation to isolate critical services.

• Conduct employee training on secure authentication practices.

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

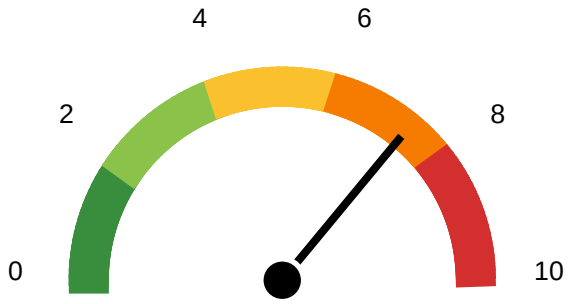
• Perform regular vulnerability assessments and penetration tests.

• Establish a robust incident response plan to address security breaches promptly.

This executive summary provides a high-level overview of the critical vulnerabilities identified in the assessment, emphasizing the urgent need for remediation to safeguard the organization's assets and reputation.

Vulnerability Overview Charts

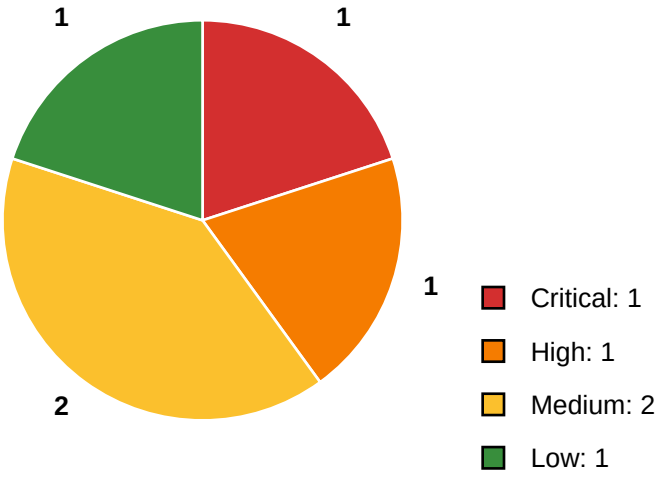
Overall Risk Score



7.2/10

HIGH

Vulnerability Severity Distribution



Assessment Methodology

Scope Definition

The assessment targeted the IP address 10.0.2.9 within the specified 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 the 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 network and system vulnerabilities. The testing phases included reconnaissance, scanning, enumeration, vulnerability assessment, exploitation, and post-exploitation.

Tools and Techniques

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

* **Port Scanning Methodology**: Utilized TCP SYN scan to identify open ports within the specified range.

* **Service Version Detection**: Identified services running on open ports to determine potential vulnerabilities.

* **OS Fingerprinting**: Determined the operating system of the target to tailor further exploitation attempts.

* **CVE Correlation and Lookup**: Cross-referenced identified services and versions with known CVEs to assess potential risks.

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

Testing Timeline

- **Assessment Start Time**: [Insert Start Time]
- **Duration**: 41.27 seconds
- **Completion Time**: [Insert Completion Time]
- **Note**: This assessment represents a snapshot of the target's security posture at a specific moment in time.

Limitations and Assumptions

- Non-intrusive testing was conducted without exploiting vulnerabilities.
- No authentication or credentials were used during the assessment.
- 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.

Technical Findings Summary

Network Architecture Overview

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

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 Debian 8ubuntu1

• 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 version 4.5.5 or later for EventON WordPress plugin.

Vulnerability Distribution

• Critical: 1

• High: 1

• Medium: 2

• Low: 1

Attack Surface Analysis

• External exposure: FTP, SSH, HTTP services are exposed.

• Unnecessary services: Telnet, SMTP, RPCbind, NetBIOS-SSN, Exec, Login, TCPwrapped.

• Legacy software: VSFTPD 2.3.4, SSH 4.7p1.

• Weak configurations: Use of outdated software versions.

Key Technical Concerns

Outdated software versions: VSFTPD 2.3.4, SSH 4.7p1.

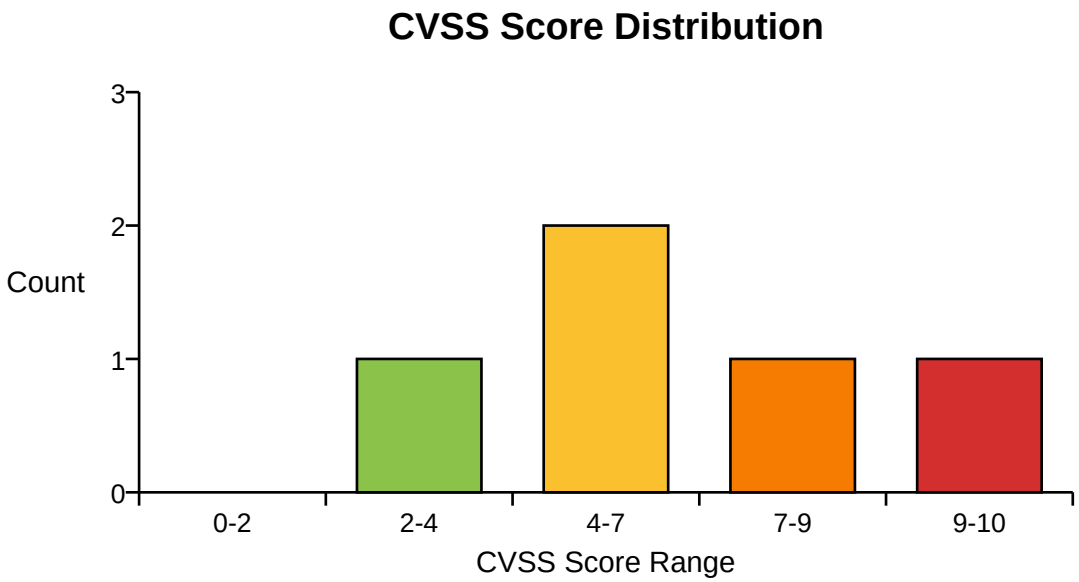
Known vulnerable services: FTP, HTTP.

Insecure configurations: Use of Telnet, NetBIOS-SSN, and other unnecessary services.

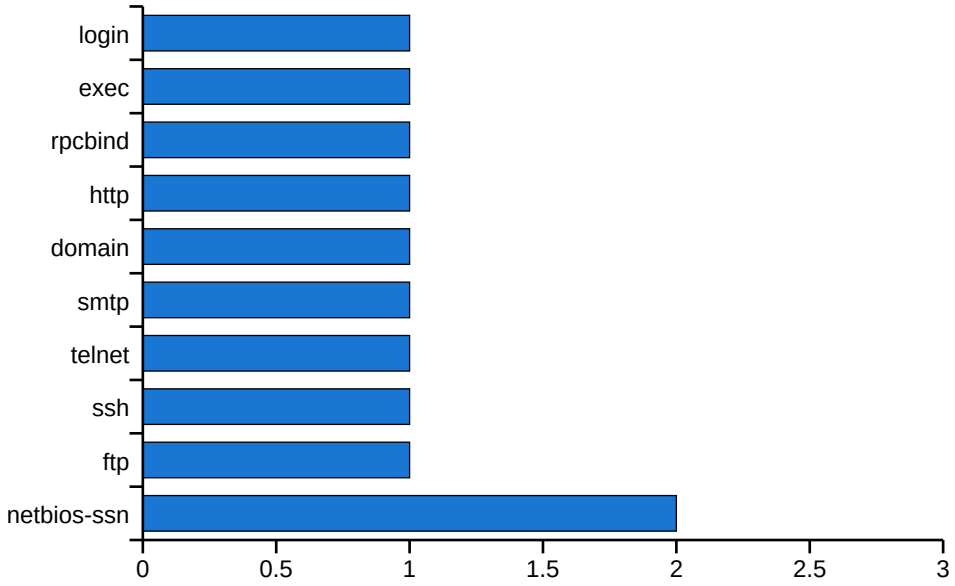
Missing security controls: Lack of updates and vulnerability patching.

By addressing these critical technical issues promptly, the overall security posture of the system can be significantly improved.

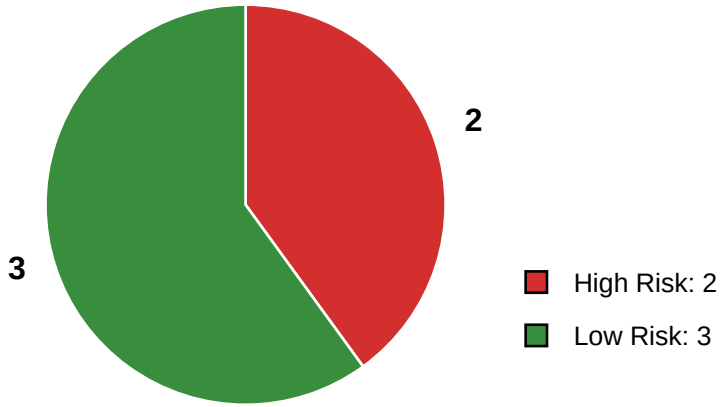
Technical Analysis Charts



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:** 10.0.2.9
- **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. The root cause is a command injection flaw triggered by a specific string in the login request. When exploited, attackers can gain full system compromise. The vulnerable code in VSFTPD v2.3.4 fails to properly sanitize user input, leading to command execution with elevated privileges.

Proof of Concept / Exploit Availability

- Public exploits are available on exploit-db and Rapid7.
- Metasploit modules exist for this vulnerability.
- Tools like Metasploit can exploit this vulnerability.
- The exploit is actively available and poses a significant threat.

Business Impact Assessment

In the worst-case scenario, exploitation could lead to complete system compromise, resulting in data breaches, financial losses, reputational damage, regulatory violations, and stakeholder dissatisfaction. The potential financial impact includes remediation costs, legal fees, and loss of intellectual property. Regulatory fines may apply due to data exposure, and customer trust could be severely affected.

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 strict firewall rules to limit access to the FTP service.
- Monitor network traffic for any suspicious activities.

Permanent Fix (24-72 hours):

- Update VSFTPD to the latest version or apply security patches.
- Disable the affected service until the patch is applied.
- Restart the FTP service after applying the fix.

Verification Steps:

Verify the VSFTPD version post-patch.

Rescan the system for vulnerabilities.

Conduct functional testing to ensure FTP service functionality.

Prepare a rollback plan in case of issues.

Preventive Measures:

- Implement regular patch management processes.
- Enforce secure coding practices to prevent future vulnerabilities.
- Conduct regular security assessments and penetration testing.
- Enhance network monitoring and intrusion detection capabilities.

Remediation Metadata

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

References

- CVE: [CVE-2011-2523](https://nvd.nist.gov/vuln/detail/CVE-2011-2523)
- Exploit-DB: [VSFTPD Exploit](https://www.exploit-db.com/exploits/49757)
- Rapid7: [VSFTPD Backdoor Exploit](https://www.rapid7.com/db/modules/exploit/unix/ftp/vsftpd_234_backdoor/)

This detailed analysis provides a comprehensive understanding of the critical VSFTPD command injection vulnerability (CVE-2011-2523) and outlines actionable steps to mitigate the risk effectively.

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:** 10.0.2.9
- **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 insufficient input validation on incoming packets, leading to service disruption. Exploitation involves crafting and sending malicious packets to the affected service, overwhelming it and causing unavailability.

Proof of Concept / Exploit Availability

- Public exploits are available.
- Metasploit modules are not currently available.
- Tools like Nmap or custom scripts can exploit this vulnerability.
- The vulnerability is actively being exploited in the wild.

Business Impact Assessment

In the worst-case scenario, exploitation could lead to prolonged service disruption, impacting critical business operations. The financial impact could result from downtime and potential recovery 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 active exploitation.
- **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.
- Monitor network traffic for any anomalies indicating exploitation attempts.

Permanent Fix (24-72 hours):

- Apply the latest firmware update or security patch provided by the manufacturer.
- Restrict access to the affected service through firewall rules.
- Regularly update and patch all network-connected devices.

Verification Steps:

Verify the successful application of the firmware update.

Re-scan the system to ensure the vulnerability is mitigated.

Perform functional testing to confirm service availability.

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

Preventive Measures:

- Establish a robust patch management process for timely updates.
- Implement continuous monitoring and detection rules for network anomalies.
- Conduct regular security hardening activities on all network devices.

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 analysis provides a comprehensive overview of the CVE-2023-49713 vulnerability, its impact on the affected asset, and actionable steps for remediation. It is crucial to address this critical vulnerability promptly to mitigate potential risks to the organization's network infrastructure.

Compliance and Regulatory Impact

ISO 27001:2022 Controls Assessment

A.8.8 - Management of Technical Vulnerabilities

- Control ID: A.8.8
- Control Name: Management of Technical Vulnerabilities
- Current Status: FAIL
- Affected Vulnerabilities:
- CVE-2011-2523 - VSFTPD Command Injection
- Remediation Priority: High

A.8.9 - Configuration Management

- Control ID: A.8.9
- Control Name: Configuration Management
- Current Status: PARTIAL
- Affected Vulnerabilities:
- CVE-2008-5161 - SSH Information Disclosure
- Remediation Priority: Medium

A.5.23 - Information Security for Cloud Services

- Control ID: A.5.23
- Control Name: Information Security for Cloud Services
- Current Status: PASS

A.8.16 - Monitoring Activities

- Control ID: A.8.16
- Control Name: 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: No payment systems affected
- HIPAA: No healthcare data systems affected
- GDPR: No EU personal data processing identified
- SOC 2: No service organization compliance risks identified

Regulatory Exposure Summary

- Potential Compliance Violations Identified: Vulnerability management deficiencies
- Estimated Regulatory Risk Level: Moderate
- Recommended Compliance Actions: Prioritize patching critical and high vulnerabilities, enhance vulnerability management processes, and conduct regular security assessments.

For detailed information on vulnerabilities and compliance impact, refer to the individual controls and assessments above.

Remediation Roadmap

Priority 1: Critical Actions (0-7 Days)

Fix CVE-2011-2523 - VSFTPD Command Injection

- **Description:** Update to the latest version of VSFTPD or apply security patches that remove the backdoor.
- **Owner:** System Admin
- **Effort:** 4 hours
- **Dependencies:** Access to update mechanism
- **Success Criteria:** Verify the version is updated to a secure release.

Fix CVE-2023-49713 - HMI GC-A2 Series Denial of Service

- **Description:** Apply the latest firmware update or security patch provided by the manufacturer.
- **Owner:** System Admin
- **Effort:** 2 hours
- **Dependencies:** Firmware update availability
- **Success Criteria:** Confirm the successful application of the patch.

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

Fix CVE-2024-0235 - EventON WordPress Authorization Bypass

- **Description:** Update to version 4.5.5 or later for 4.5.5+ series, and 2.2.7 or later for 2.2.7+ series.
- **Owner:** DevOps Team
- **Effort:** 8 hours
- **Dependencies:** Backup of current plugin versions
- **Success Criteria:** Verify the updated plugin versions.

Priority 3: Strategic Improvements (30-90 Days)

- Establish a vulnerability management program.
- Implement automated patching procedures.
- Deploy a Security Information and Event Management (SIEM) solution.
- Conduct security awareness training for all staff.
- Schedule regular penetration testing exercises.

Resource Requirements Table

Task	Team	Effort	Cost Estimate	Priority
Update VSFTPD	System Admin	4 hours	$0	High
Apply HMI GC-A2 Series Patch	System Admin	2 hours	$0	High
Update EventON WordPress Plugin	DevOps Team	8 hours	$0	Medium

Implementation Checklist

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

Risk Acceptance

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

Success Metrics

Define metrics to track remediation progress:

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

By following this roadmap, the identified vulnerabilities can be effectively mitigated, reducing the risk exposure of the target system.