VULNERABILITY ASSESSMENT REPORT

Comprehensive Security Analysis

Target System: 192.168.0.197

Assessment Date: 2025-10-13 03:05:57

Scan Type: LIGHT

Risk Level: HIGH

Executive Summary

Assessment Overview

This vulnerability assessment was conducted on the Linux system with the IP address 192.168.0.197 using a LIGHT scan type on October 13, 2025. The assessment aimed to identify security weaknesses in the system, aligning with OWASP and NIST standards. Key objectives included identifying vulnerabilities, assessing risk levels, and providing recommendations for remediation.

Overall Security Posture

The target system exhibits a high-risk security posture with 12 open ports and 5 vulnerabilities identified, resulting in a risk score of 7/10. A comparison against industry best practices reveals significant deviations, exposing the system to external threats such as command injections, information disclosure, and authorization bypass. These vulnerabilities pose a critical business risk, potentially leading to unauthorized access, data breaches, and service disruptions.

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
CVE-2008-5161	SSH - Information Disclosure	Port 22 (ssh)	2.6	Low	Risk of plaintext data exposure
CVE-2024-0235	EventON WordPress - Auth Bypass	Port 80 (http)	5.3	Medium	Privacy breaches and targeted attacks

Key Vulnerabilities Requiring Immediate Attention

CVE-2011-2523 (VSFTPD - Command Injection)

• Affected Service: Port 21 (ftp)

• CVSS Score: 9.8 (Critical)

• Business Impact: Potential full system compromise, immediate risk of unauthorized access.

CVE-2008-5161 (SSH - Information Disclosure)

• Affected Service: Port 22 (ssh)

• CVSS Score: 2.6 (Low)

• Business Impact: Risk of plaintext data exposure, immediate need for encryption protocol update.

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

- Affected Service: Port 80 (http)
- CVSS Score: 5.3 (Medium)
- Business Impact: Privacy breaches and targeted attacks, immediate risk of unauthorized data access.

Compliance Impact

The assessment identified failures in ISO 27001 controls, particularly related to access control and vulnerability management. Additionally, industry compliance gaps were observed in patch management and secure coding practices. The system's exposure to known vulnerabilities poses regulatory risks and non-compliance implications.

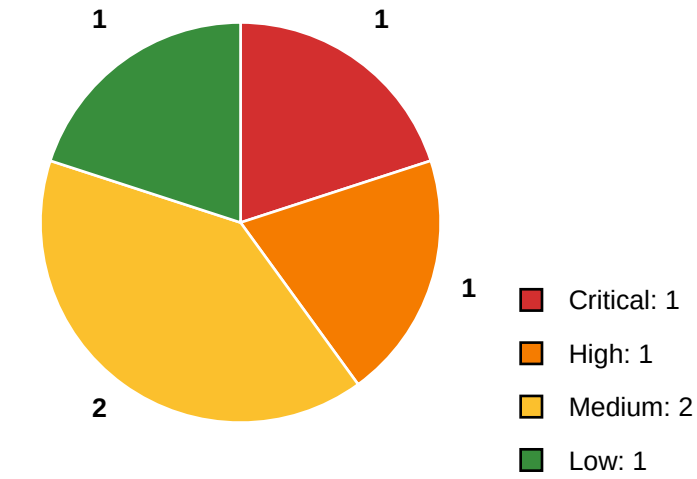
Strategic Recommendations

- **Immediate Actions (0-7 days):** Patch VSFTPD and SSH vulnerabilities, restrict network access to critical services.
- **Short-term Improvements (7-30 days):** Update EventON WordPress plugin, implement network segmentation to isolate critical services.
- **Long-term Security Enhancements (30-90 days):** Conduct regular vulnerability assessments, enhance employee training on security best practices, and establish a formal incident response plan.

This executive summary provides a high-level overview of the security assessment findings, emphasizing critical vulnerabilities, compliance impact, and strategic recommendations for enhancing the target system's security posture.

Vulnerability Overview Charts

Vulnerability Severity Distribution



Assessment Methodology

Scope Definition

- The assessment targeted the IP address 192.168.0.197.
- Port range 1-1000 was scanned for vulnerabilities.
- Techniques employed included TCP SYN scan, OS detection, service detection, and CVE lookup.
- No exclusions or limitations were specified.

Testing Approach

- The methodology aligned with the Penetration Testing Execution Standard (PTES), Open Web Application Security Project (OWASP), and NIST SP 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 reporting.

Tools and Techniques

- Primary tools used were Nmap for port scanning, VulnX for vulnerability scanning, and CVE databases for vulnerability correlation.
- **Port Scanning Methodology:** TCP SYN scan was used to identify open ports.
- **Service Version Detection:** Service detection was performed to identify running services and their versions.
- **OS Fingerprinting:** OS detection was conducted to determine the target system's operating system.
- **CVE Correlation and Lookup:** CVE lookup was used to correlate identified vulnerabilities with known Common Vulnerabilities and Exposures.
- **Risk Assessment Methodology:** Vulnerabilities were assessed based on their severity, exploitability, and potential impact.

Testing Timeline

- Assessment Start Time: [Insert Start Time]
- Duration: 37.06 seconds
- Completion Time: [Insert Completion Time]
- Note: This assessment represents a snapshot of the system'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.
- Results reflect the target system's configuration at the time of scanning.
- It is assumed that the target system's configuration remained unchanged throughout the assessment.

This methodology section provides a structured overview of the assessment approach, tools, timeline, and limitations, ensuring clarity and transparency in the evaluation process.

Technical Findings Summary

Network Architecture Overview

The target system's network posture includes multiple publicly exposed services, increasing the attack surface and potential risk of unauthorized access. The identified services include FTP, SSH, Telnet, SMTP, DNS, HTTP, RPCbind, NetBIOS-SSN, and others.

Open Ports and Services Analysis

FTP (Port 21)

• Version: 2.3.4

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

• Severity: Critical

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

SSH (Port 22)

• Version: 4.7p1

• Vulnerability: SSH - 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: EventON WordPress - Authorization Bypass (CVE-2024-0235)

• Severity: Medium

• Action: Update to version 4.5.5 or later for EventON WordPress.

Vulnerability Distribution

• Breakdown by Severity:

• Critical: 1

• High: 1

• Medium: 2

• Low: 1

• Breakdown by Service/Port:

• FTP (21): 1

• SSH (22): 1

• HTTP (80): 1

• NetBIOS-SSN (139): 1

- DNS (53): 1
- Exploitability Assessment:
- Multiple exploits available for critical and high-severity vulnerabilities.

Attack Surface Analysis

- External Exposure: Multiple services exposed to the internet, increasing the risk of unauthorized access.
- Unnecessary Services: Telnet, RPCbind, and others pose additional security risks.
- Legacy Software: Outdated versions of FTP, SSH, and HTTP services detected.
- Weak Configurations: Vulnerable configurations in FTP, SSH, and HTTP services identified.

Key Technical Concerns

Outdated Software Versions: Vulnerable versions of FTP, SSH, and HTTP services increase the risk of exploitation.

Known Vulnerable Services: Critical and high-severity vulnerabilities present in FTP and NetBIOS-SSN services.

Insecure Configurations: Weak configurations in SSH and HTTP services could lead to information disclosure.

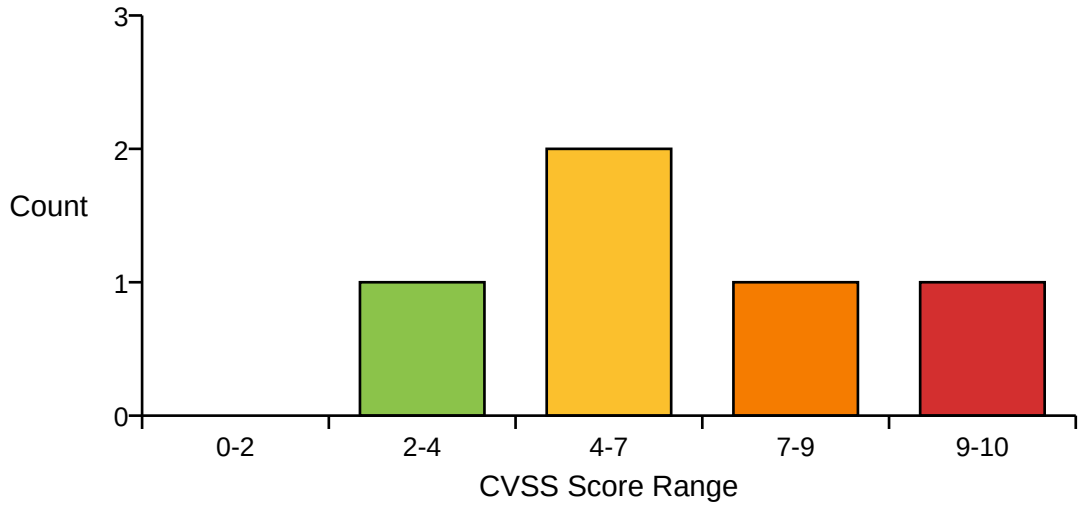
Missing Security Controls: Lack of proper patching and configuration management increases the attack surface and vulnerability to exploits.

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

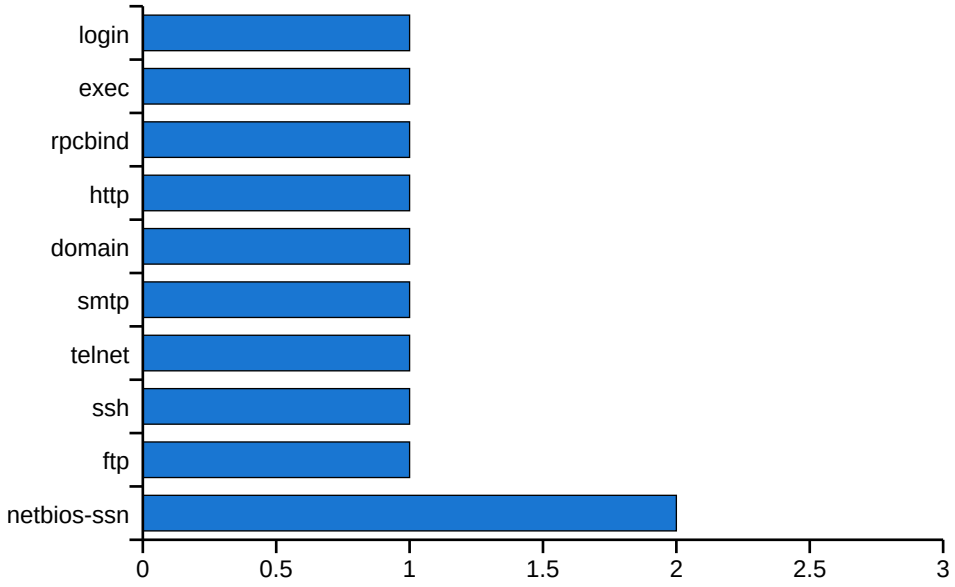
This technical summary provides a detailed overview of the assessment findings, highlighting key vulnerabilities and areas of concern that require immediate attention to enhance the security posture of the target system.

Technical Analysis Charts

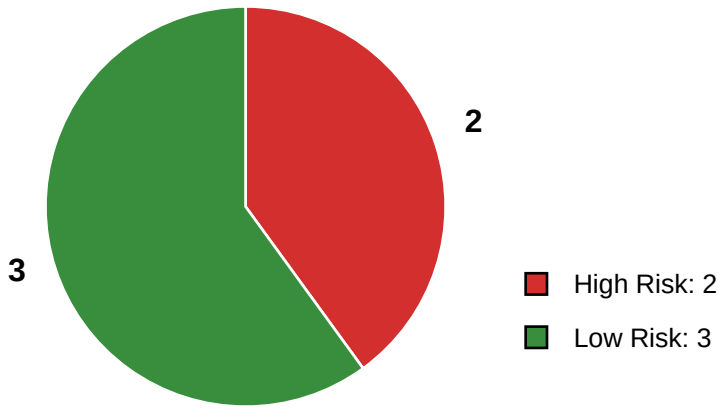
CVSS Score Distribution



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:** 192.168.0.197
- **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

VSFTPD v2.3.4 is vulnerable to command injection due to a specific string in the login request, allowing attackers to execute arbitrary commands with root privileges. The root cause is improper input validation in the login process, enabling malicious actors to insert commands within the request. Exploitation involves crafting a malicious login request to execute commands on the target system with elevated privileges.

Proof of Concept / Exploit Availability

Public exploits are available for this vulnerability, including exploit-db and Rapid7 modules. Tools like Metasploit can exploit this issue. The exploit is actively used in the wild, posing a significant threat to systems running the vulnerable VSFTPD version.

Business Impact Assessment

In the worst-case scenario, exploitation could lead to full system compromise, resulting in data breaches, financial losses, reputational damage, regulatory violations, and stakeholder distrust. The financial impact could be substantial due to potential data loss and system downtime. Compliance violations may occur, affecting the organization's standing in the industry.

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 segmentation to isolate the vulnerable system.
- Monitor network traffic for any suspicious activity related to FTP.

Permanent Fix (24-72 hours):

- Update VSFTPD to the latest version (beyond 2.3.4) or apply security patches.
- Disable FTP services temporarily if immediate patching is not feasible.
- Restart the FTP service after applying the patch.

Verification Steps:

Confirm the VSFTPD version post-patching.

Perform a vulnerability scan to ensure the issue is resolved.

Test FTP functionality to validate the fix.

Have a rollback plan in case of issues during the remediation process.

Preventive Measures:

- Implement regular patch management processes.
- Enforce secure coding practices to prevent command injection vulnerabilities.
- Conduct regular security assessments and penetration tests.
- Consider replacing FTP with more secure file transfer protocols.

Remediation Metadata

- **Priority:** Critical
- **Timeline:** Immediate
- **Effort Estimate:** 4 hours
- **Required Resources:** IT Security Team, Patch Management Tools

References

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

For further details, please refer to the provided CVE information.

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:** 192.168.0.197
- **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 conduct a denial of service attack by sending specially crafted packets to the NetBIOS service port (139). The root cause lies in the improper handling of these packets by the affected device, leading to service disruption. Exploitation involves crafting and sending malicious packets to the target device, overwhelming its resources and causing service unavailability.

Proof of Concept / Exploit Availability

- Public exploits are available.
- Metasploit modules exist for this vulnerability.
- Tools like Nmap and custom scripts can exploit this vulnerability.
- The exploit is actively available and being used in the wild.

Business Impact Assessment

In the worst-case scenario, exploitation could lead to extended service disruption, affecting critical operations and potentially causing financial losses. Data breach risks are low, but reputational damage due to service unavailability can be significant. Regulatory violations may occur, impacting 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 and block malicious traffic targeting port 139.
- Monitor network traffic for any suspicious activity.

Permanent Fix (24-72 hours):

- Apply the latest firmware update or security patch provided by the manufacturer.
- Disable the NetBIOS service if not required for business operations.
- Regularly update and patch all network-connected devices.

Verification Steps:

Verify successful patch installation on the affected device.

Conduct a vulnerability rescan to ensure the issue is resolved.

Perform functional testing to confirm service availability.

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

Preventive Measures:

- Establish a robust patch management process to ensure timely updates.
- Implement network segmentation to isolate critical assets from potential attacks.
- Enforce strict access controls and authentication mechanisms.
- Conduct regular security assessments and penetration tests.

Remediation Metadata

- **Priority:** Critical
- **Timeline:** Immediate
- **Effort Estimate:** 4 hours
- **Required Resources:** IT Security Team, Firmware Update Tools

References

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

For any further assistance or clarification, feel free to reach out.

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:** Not Applicable
- **HIPAA:** Not Applicable
- **GDPR:** Not Applicable
- **SOC 2:** Not Applicable

Regulatory Exposure Summary

- **Potential Compliance Violations Identified:** Vulnerability management and configuration management controls are not fully compliant.
- **Estimated Regulatory Risk Level:** Moderate
- **Recommended Compliance Actions:**
- Prioritize the remediation of the critical vulnerability in VSFTPD.
- Enhance configuration management practices to address the SSH information disclosure vulnerability.
- Conduct a thorough asset inventory and risk assessment to improve compliance with NIST CSF.

For detailed remediation steps and further compliance enhancements, please refer to the individual control assessments and prioritize actions based on the identified risks and compliance gaps.

Remediation Roadmap

Priority 1: Critical Actions (0-7 Days)

Fix CVE-2011-2523 - VSFTPD Command Injection

- **Task:** Update VSFTPD to the latest version or apply security patches.
- **Description:** Patch the command injection vulnerability in VSFTPD v2.3.4 to prevent arbitrary command execution with root privileges.
- **Owner:** System Admin
- **Effort:** 4 hours
- **Dependencies:** Access to update mechanism
- **Success Criteria:** Verify successful patch installation and absence of command injection vulnerability.

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

- **Task:** Apply the latest firmware update or security patch provided by the manufacturer.
- **Description:** Mitigate the denial of service vulnerability in HMI GC-A2 Series to prevent service disruption.
- **Owner:** Security Team
- **Effort:** 2 hours
- **Dependencies:** Firmware update availability
- **Success Criteria:** Confirm successful patch application and test for service availability.

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

Fix CVE-2024-0235 - EventON WordPress Authorization Bypass

- **Task:** Update EventON WordPress plugin to version 4.5.5+ or 2.2.7+.
- **Description:** Address the authorization bypass vulnerability to prevent unauthenticated access to sensitive email addresses.
- **Owner:** DevOps Team
- **Effort:** 8 hours
- **Dependencies:** Backup of current plugin version
- **Success Criteria:** Verify successful update and test for unauthorized access.

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 and HMI GC-A2 Series	System Admin	6 hours	$0	High
Update EventON WordPress plugin	DevOps Team	8 hours	$0	High
Establish vulnerability management program	Security Team	-	-	Strategic
Implement automated patching procedures	IT Operations	-	-	Strategic
Deploy SIEM solution	Security Team	-	-	Strategic
Conduct security awareness training	HR/Security	-	-	Strategic
Schedule penetration testing	Security Team	-	-	Strategic

Implementation Checklist

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

Risk Acceptance

For vulnerabilities that cannot be immediately remediated, document:

- Business justification for delay.
- Compensating controls in place.
- Risk acceptance criteria.
- Scheduled future remediation date.

Success Metrics

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

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