VULNERABILITY ASSESSMENT REPORT

SMB Network & Endpoint Security Assessment

Client	Acme Manufacturing LLC [Sanitized — Client Confidential]
Assessment Type	Internal Network & Endpoint Vulnerability Assessment
Scope	10.0.0.0/24 internal network — 47 hosts; 3 Windows Server instances; workstations; network devices
Engagement Date	Q1 2026
Prepared By	Kevin Leverett | Converged Security Consulting
Classification	CONFIDENTIAL — For Authorized Recipients Only

1. Executive Summary

A vulnerability assessment was conducted against the internal network and endpoints of the client environment. The assessment was performed using industry-standard tools and methodologies aligned with the NIST SP 800-115 Technical Guide to Information Security Testing and Assessment.

The assessment identified 14 vulnerabilities across the scoped environment, including 2 Critical findings that require immediate remediation. The most significant risks involve an unpatched Windows Server with a known remote code execution vulnerability, exposed administrative interfaces accessible without multi-factor authentication, and outdated endpoint software across 60% of workstations.

Remediation of the Critical and High findings is strongly recommended prior to any further network expansion or external-facing service deployment.

Finding Summary

Severity	Count	Remediated	Accepted Risk
Critical	2	0	0
High	4	0	0
Medium	5	2	1
Low	3	1	0
Total	**14**	**3**	**1**

2. Scope & Methodology

2.1 Scope of Assessment

The assessment was limited to the following in-scope targets, as defined in the signed Rules of Engagement document:

- Internal network segment: 10.0.0.0/24 (47 active hosts identified)
- Windows Server 2016 (x2) and Windows Server 2019 (x1)
- Employee workstations: Windows 10/11 (32 hosts)
- Network infrastructure: 2 managed switches, 1 firewall appliance, 1 wireless access point
- Web application: Internal HR portal (192.168.1.50:8080)

2.2 Out of Scope

- Production database servers (excluded per client request)
- Third-party SaaS applications
- Physical security controls (covered under separate engagement)

2.3 Methodology

The assessment followed a structured four-phase approach consistent with NIST SP 800-115 and industry best practices:

Phase	Activity	Tools / Techniques
1	Reconnaissance & Discovery	Nmap host discovery, port scanning, OS fingerprinting
2	Vulnerability Scanning	OpenVAS authenticated & unauthenticated scans; Nessus plugin checks
3	Analysis & Validation	Manual validation of scanner findings; CVSS v3.1 scoring; MITRE ATT&CK mapping
4	Reporting	Executive summary, technical findings, risk-ranked remediation roadmap

3. Detailed Findings

Each finding is assigned a CVSS v3.1 base score and mapped to the relevant MITRE ATT&CK technique where applicable. Remediation priority reflects both CVSS score and business context.

3.1 [CRITICAL] Unpatched RCE Vulnerability — Windows Server 2016

Field	Detail
CVE	CVE-2023-XXXX (sanitized)
CVSS Score	9.8 (Critical)
Affected Host	192.168.1.10 (WIN-SRV-01)
ATT&CK Technique	T1190 — Exploit Public-Facing Application
Description	Windows Server 2016 running without the most recent cumulative update patch, exposing a known remote code execution vulnerability exploitable over the network without authentication.

Remediation	Apply latest Windows cumulative update immediately. Isolate host from network until patched. Verify patch deployment via WSUS or SCCM.
Priority	**IMMEDIATE — within 24 hours**

3.2 [CRITICAL] Admin Interface Without MFA — Firewall Management Console

Field	Detail
CVE	CWE-308 — Use of Single-Factor Authentication
CVSS Score	9.1 (Critical)
Affected Host	192.168.1.1 (Firewall Admin Console — Port 443)
ATT&CK Technique	T1078 — Valid Accounts / T1110 — Brute Force
Description	The firewall management console is accessible on the internal network using only a username and password with no MFA requirement. Default admin credentials were confirmed unchanged from factory defaults.
Remediation	Enable MFA on management console immediately. Change all default credentials. Restrict console access by IP whitelist to administrator workstations only.
Priority	**IMMEDIATE — within 24 hours**

3.3 [HIGH] Outdated Endpoint Software — 60% of Workstations

Field	Detail
CVSS Score	7.5 (High)
Affected Hosts	19 of 32 workstations running outdated browser, Office, or AV definitions
ATT&CK Technique	T1203 — Exploitation for Client Execution
Description	A significant portion of the workstation fleet is running outdated software versions with known publicly-disclosed vulnerabilities. AV definition age ranges from 14 to 47 days behind current.
Remediation	Implement centralized patch management (e.g., WSUS, Intune). Enforce auto-update policies for browsers and Office applications. Automate AV definition updates daily.
Priority	**Within 7 days**

4. Risk Summary & Remediation Roadmap

The following roadmap prioritizes remediation actions based on severity, exploitability, and potential business impact. Items are grouped into three action windows:

Timeline	Finding	Recommended Action	Severity

24 hrs	Unpatched Windows Server RCE	Patch immediately; isolate if patch not yet available	Critical
24 hrs	Firewall admin — no MFA, default creds	Enable MFA, change credentials, restrict by IP	Critical
7 days	Outdated endpoint software (60% of fleet)	Deploy centralized patch management; enforce update policies	High
7 days	SMBv1 enabled on 3 servers	Disable SMBv1; enable SMBv2/v3 with signing required	High
30 days	Weak password policy (no complexity enforcement)	Implement domain-level password policy; consider password manager	Medium
30 days	Unencrypted internal web application traffic (HTTP)	Enforce HTTPS on internal HR portal; deploy internal CA cert	Medium
60 days	No centralized logging / SIEM integration	Deploy log aggregation (Splunk free tier or Sentinel); establish baseline alerting	Low

5. Conclusion & Recommendations

The assessment identified a meaningful attack surface within the client environment, concentrated primarily in patch management deficiencies and authentication control gaps. The two Critical findings represent the most immediate risk — an attacker with network access could leverage either vulnerability to gain unauthorized administrative control over core infrastructure.

Implementing the 24-hour remediation actions and following the 30-day roadmap will significantly reduce the organization's exploitable attack surface. A follow-up verification scan is recommended 30 days after remediation of Critical and High findings to confirm closure.

Long-term, the organization would benefit from:

- A formal vulnerability management program with quarterly scan cadence
- SIEM deployment for centralized visibility and anomaly detection
- Security awareness training for all employees (phishing simulation recommended)
- Documented incident response plan aligned to NIST SP 800-61

Prepared by: Kevin Leverett | Converged Security Consulting
Contact: k.leverett32@gmail.com | (850) 774-2218 | Charlotte, NC (Remote Available)
All assessments performed under signed authorization agreement only. Unauthorized testing is prohibited under the CFAA.