ClearSight Security LLC

Vulnerability Assessment Report -- SAMPLE

Building better security, one assessment at a time.

SAMPLE REPORT -- NOT A REAL CLIENT
FINDINGS SHOWN ARE FICTIONAL DEMONSTRATION DATA

Client: Example Business Group (SAMPLE - fictional client)
Report Date: November 17, 2026
Total Findings: 4
Severity Summary: 1 Critical | 2 High | 1 Medium | 0 Low

Executive Summary

Our assessment of your business's IT security has identified a total of 4 findings. The risk picture is as follows: 1 critical, 2 high, and 1 medium severity findings.

The most pressing issue is the presence of default credentials on the admin panel, which is a critical finding. Additionally, we found that no multi-factor authentication is enabled on email accounts, which is a high severity finding.

No known-exploited vulnerabilities were found (checked against the CISA Known Exploited Vulnerabilities catalog, version 2026.11.10).

The Regulatory Context section shows which findings relate to the areas addressed by frameworks that may apply to this client, as technical context. It is not a compliance determination - see Scope & Limitations at the end of this report.

Methodology

Findings are identified through automated scanning and vulnerability databases (NVD, CISA KEV, EPSS), then reviewed and interpreted by the assessor.

What To Fix First

Recommended order, based on whether a weakness is being actively exploited (CISA KEV), its severity, its likelihood of exploitation (EPSS) and its risk score.

1) Default Credentials on Admin Panel (finding #1) - Critical severity; risk score 9/10

SAMPLE

Default credentials on the admin panel are exposed, which means anyone can access the panel without a password, posing a significant risk to the business's sensitive data and operations.

2) No MFA on Email Accounts (finding #2) - High severity; risk score 8/10; equal priority with #3

No multi-factor authentication (MFA) is enabled on email accounts, making it easier for attackers to gain unauthorized access to sensitive information and potentially disrupt business operations.

3) Unsupported Windows Version (Windows 10, end of support) (finding #3) - High severity; risk score 8/10; equal priority with #2

The Windows 10 operating system is no longer supported, which means it will not receive security updates, leaving the system vulnerable to known security threats and potentially causing data loss or system crashes.

4) Weak SSL/TLS Configuration on Web Portal (finding #4) - Medium severity; risk score 5/10

The SSL/TLS configuration on the web portal is weak, which could allow attackers to intercept sensitive information, such as login credentials or financial data, and potentially compromise the business's online presence.

Assessment Scope

Network Segments / Hosts Assessed: Office

Hosts Identified: 192.0.2.1, 192.0.2.20, 192.0.2.45, 192.0.2.80
Assessment Type: White-box / passive vulnerability assessment
Point-in-Time: November 17, 2026
Vulnerability Data Sources

CISA KEV catalog: version 2026.11.10, released 2026-11-10 - verified as the latest published version on 2026-11-12

NVD CVE data: data as of 2026-11-10

last verified 2026-11-11

Exploit-DB: package 20261027-0kali1 (2026-10-27)

KEV file SHA-256: 41C8091AD62D508D6F8906AD5CD26B20

EFE551F7D51B95ECC8A6981FA640B4EA

NVD dataset SHA-256: E88B1145AB47E3BD497FF16D8696EF6A

1258AAA199791C5417FEBCF6F151811F

(over the NVD-published hashes of the 26 imported feeds)

Data check performed: 2026-11-12

FIRST EPSS scores: dated 2026-11-16 (406,741 CVEs scored)

Scanned Hosts

SAMPLE

Addresses scanned: 254

Hosts responding: 11

Hosts with open ports: 4

Open-port hosts examined: 192.0.2.1, 192.0.2.20, 192.0.2.45, 192.0.2.80

- Office: target 192.0.2.0/24; 254 scanned, 11 responding, 4 with open ports

(scanned Tue Nov 17 04:47:20 2026)

Findings (Prioritized By Severity)

1. [CRITICAL] Default Credentials on Admin Panel

Risk Score: 9/10

Location: Office [network] (IP: 192.0.2.1)

Detected by: DEMO DATA (fictional)

Description: [DEMO] The router's web admin panel accepted the factory-default login (admin / admin). Anyone on the network could change firewall, DNS and Wi-Fi settings or lock the business out of its own network.

What this means for your business:

The security assessment found that the admin panel for your router has default login credentials, which means anyone on your network could log in without a password. This is a problem because it allows someone to change important settings, like the firewall and Wi-Fi, or even lock you out of your own network. This is a critical risk to your business because it could give unauthorized access to your network and potentially disrupt your operations.

Suggested Remediation:

1. Change the default admin login credentials to a strong password, and make sure to use a unique combination of characters, numbers, and symbols. You can ask your internet service provider for help with this.
2. Update the admin login credentials to something other than 'admin' and 'admin', and make sure to use a strong password policy that includes a minimum of 12 characters, mixed case, numbers, and symbols. You can ask your internet service provider for help with this.
3. Enable multi-factor authentication (MFA) on the admin account to add an extra layer of security. You can ask your internet service provider for help with this.

2. [HIGH] No MFA on Email Accounts

SAMPLE

Risk Score: 8/10

Location: Office [cloud service] (IP: 192.0.2.20)

Detected by: DEMO DATA (fictional)

Description: [DEMO] Staff email accounts, including the owner's administrator account, sign in with a password only. A single phished or reused password gives an attacker the mailbox, password resets for other services, and a trusted address for invoice fraud.

What this means for your business:

Your staff's email accounts, including your own administrator account, only use a password to sign in. This means that if someone gets your password, they can access your email and potentially use it to reset passwords for other services or send fake invoices to your business. If an attacker gets control of your email, it could lead to serious problems for your business.

Suggested Remediation:

1. Contact your email provider to enable Multi-Factor Authentication (MFA) on all staff email accounts, including the owner's administrator account.
2. Reach out to your email provider to require MFA for remote access to the email service.
3. Save a copy of the MFA recovery codes provided by your email provider in a secure location, such as a locked cabinet or a password-protected document.
4. Test the MFA login process for each staff email account to ensure it's working correctly.

3. [HIGH] Unsupported Windows Version (Windows 10, end of support)

Risk Score: 8/10

Location: Office [workstation] (IP: 192.0.2.45)

Detected by: DEMO DATA (fictional)

Description: [DEMO] The front-desk workstation runs Windows 10, which no longer receives security updates from Microsoft. Newly discovered vulnerabilities on this machine will never be patched.

What this means for your business:

Your front-desk workstation is running an old version of Windows 10, which means it's no longer getting important security updates from Microsoft. This makes it vulnerable to new security threats that can't be

SAMPLE

fixed. If a hacker finds a weakness in this outdated system, your business could be at risk of a security breach.

Suggested Remediation:

1. Contact Microsoft or a certified IT provider to plan and execute the migration to a supported Windows version, such as Windows 11.
2. Until the workstation is upgraded, move it to a separate network segment with limited access to the rest of the office network, to reduce potential damage from any existing vulnerabilities.
3. Reach out to the workstation's manufacturer or a trusted IT provider to apply any available vendor-specific mitigations and tighten access controls on the machine, to minimize potential risks.

4. [MEDIUM] Weak SSL/TLS Configuration on Web Portal

Risk Score: 5/10

Location: Office [server] (IP: 192.0.2.80)

Detected by: DEMO DATA (fictional)

Description: [DEMO] The customer web portal still accepts TLS 1.0 and TLS 1.1 and offers weak cipher suites, which lowers the protection on logins and data sent to the portal.

What this means for your business:

Your web portal's security is not as strong as it should be. It's allowing older and less secure ways of encrypting data to be used, which makes it easier for hackers to intercept sensitive information like login credentials. This could put your business's customers' personal data at risk if it's accessed by unauthorized people.

Suggested Remediation:

1. Contact your email provider or IT provider to help you update your server's SSL/TLS configuration to only use TLS 1.2 and above, which is the most secure option.
2. Work with your IT provider to disable weak cipher suites, such as RC4 and DES, to prevent hackers from exploiting them.
3. Replace your self-signed SSL certificate with a valid, trusted one from a reputable certificate authority, such as GlobalSign or DigiCert, to ensure secure connections to your web portal.
4. Have your IT provider add the HSTS header to your web portal's HTTP headers to help prevent SSL stripping attacks.

Regulatory Context

Profile: General / SMB

SAMPLE

The framework below is a widely used, non-regulatory reference for organizing security controls. It is provided as general context for an organization without a sector-specific framework. ClearSight does NOT determine which apply to this client, and does NOT assert that any finding in this report constitutes a violation. That determination requires a qualified compliance advisor or legal counsel. The table below shows which findings in this report relate to the area each control addresses.

NIST Cybersecurity Framework (CSF) 2.0:

- NIST CSF 2.0 PR.AA-01: Identities and credentials for authorized users, services, and hardware are managed -- Related findings: #1
- NIST CSF 2.0 PR.AA-03: Users, services, and hardware are authenticated -- Related findings: #1, #2
- NIST CSF 2.0 PR.AA-05: Access permissions are managed, incorporating least privilege and separation of duties -- Related findings: none observed in this assessment
- NIST CSF 2.0 PR.DS-01: The confidentiality, integrity, and availability of data-at-rest are protected -- Related findings: none observed in this assessment
- NIST CSF 2.0 PR.DS-02: The confidentiality, integrity, and availability of data-in-transit are protected -- Related findings: #4
- NIST CSF 2.0 PR.PS-01: Configuration management practices are established and applied -- Related findings: none observed in this assessment
- NIST CSF 2.0 PR.PS-02: Software is maintained, replaced, and removed commensurate with risk -- Related findings: #3
- NIST CSF 2.0 PR.PS-04: Log records are generated and made available for continuous monitoring -- Related findings: none observed in this assessment
- NIST CSF 2.0 PR.IR-01: Networks and environments are protected from unauthorized logical access and usage -- Related findings: none observed in this assessment
- NIST CSF 2.0 ID.AM-01: Inventories of hardware managed by the organization are maintained -- Related findings: none observed in this assessment
- NIST CSF 2.0 ID.AM-02: Inventories of software, services, and systems managed by the organization are maintained -- Related findings: none observed in this assessment
- NIST CSF 2.0 ID.RA-01: Vulnerabilities in assets are identified, validated, and recorded -- Related findings: none observed in this assessment
- NIST CSF 2.0 DE.CM-01: Networks and network services are monitored to find potentially adverse events -- Related findings: none observed in this assessment
- NIST CSF 2.0 DE.CM-09: Computing hardware and software, runtime environments, and their data are monitored to find potentially adverse events -- Related findings: none observed in this assessment

SAMPLE

- NIST Cybersecurity Framework 2.0: Voluntary guidance from the National Institute of Standards and Technology. It is not a law or regulation and carries no penalties; it is used here to organize the findings by security outcome.

- Maryland PIPA (Md. Code Ann., Com. Law Sec. 14-3501 et seq.; 14-3504): Requires reasonable security procedures for the personal information of Maryland residents, appropriate to the nature of the data and the size of the business, and sets breach-notification duties. Applies if such personal information is handled.

"Related" means the finding touches the area that control addresses. It is not a finding of non-compliance, and a control showing no related findings is not a statement that the control is met.

Scope & Limitations

This report documents the findings of a technical vulnerability assessment performed by ClearSight Security LLC. It reflects the state of the assessed systems at a single point in time and covers only the network segments and hosts listed in the Assessment Scope section.

ClearSight Security provides technical vulnerability assessment services. The Regulatory Context section of this report shows where a technical finding relates to an area addressed by a regulatory, contractual, or voluntary framework (NIST CSF, PIPA). This is provided as technical context only and is NOT a determination of compliance or non-compliance. ClearSight is not a compliance, legal, or regulatory authority. Whether any finding constitutes a violation, and any associated penalties, must be determined by the client in consultation with a qualified compliance advisor or legal counsel.

"Actively exploited" means the CVE appears in the CISA Known Exploited Vulnerabilities catalog, i.e. CISA has evidence it is being exploited in the wild. It does not mean this client's systems have been attacked.

Prepared by ClearSight Security LLC

Assessor: _____ Date: _____

SAMPLE