

# Security Assessment Report

**\*\*Generated:\*\*** 2026-02-13T14:48:56.391933Z

**\*\*Scope:\*\*** Uploaded Files Analysis

## Executive Summary

This security assessment identified 46 active vulnerability findings in Uploaded Files Analysis.

Severity Distribution:

- High Severity: 44 findings
- Medium Severity: 2 findings
- Low Severity: 0 findings

Findings include evidence-based detections with specific file locations and remediation suggestions. All findings should be reviewed by a security analyst for contextual risk assessment.

## Scope & Methodology

This assessment employed a deterministic rule-based scanning approach combined with AI-assisted analysis.

Detection Method:

- Pattern-based rule engine for vulnerability detection
- Evidence collection with exact file and line references
- Confidence scoring based on rule metadata and evidence completeness

Analysis Method:

- Local LLM (Ollama) for explanation and remediation suggestions
- Analyst review for final severity assessment
- Evidence-based validation of all findings

All findings include exact locations and evidence snippets for verification.

## Findings

### ***VULN-001: Exposed administrative or database port***

**\*\*Severity:\*\*** Medium

**\*\*Confidence:\*\*** 0.55

**\*\*Category:\*\*** Network

Affected Files:

- `azure\_notes.csv`

Locations:

- `azure\_notes.csv`

Evidence:

,

Time,Host,Service,Port,Protocol,Type,Data

2025-09-07 12:29:34 UTC,10.97.119.225,,,,host.os.nmap\_fingerprint,{:os\_vendor=>"Microsoft",  
:os\_family=>"Windows", :os\_version=>"2016", :os\_accuracy=>87}

2025

,

---

### ***VULN-002: Insecure plaintext protocol detected***

**\*\*Severity:\*\*** High

**\*\*Confidence:\*\*** 0.62

**\*\*Category:\*\*** Transport

Affected Files:

- `azure\_notes.csv`

Locations:

- `azure\_notes.csv`

Evidence:

,

Time,Host,Service,Port,Protocol,Type,Data

2025-09-08 08:45:18 UTC,10.67.108.106,http,80,tcp,nmap.nse.http-methods.tcp.80,{"output"=>"\n  
Supported Methods: OPTIONS TRACE GET HEAD POST\n Potentially ris

,

---

### ***VULN-003: Insecure plaintext protocol detected***

**\*\*Severity:\*\*** High

**\*\*Confidence:\*\*** 0.62

**\*\*Category:\*\*** Transport

Affected Files:

- `azure\_notes.csv`

Locations:

- `azure\_notes.csv`

Evidence:

,

Time,Host,Service,Port,Protocol,Type,Data

2025-09-08 08:45:18 UTC,10.80.23.183,http,80,tcp,nmap.nse.http-methods.tcp.80,{"output"=>"\n  
Supported Methods: OPTIONS TRACE GET HEAD POST\n Potentially risk

,

---

### ***VULN-004: Exposed administrative or database port***

**\*\*Severity:\*\* Medium**  
**\*\*Confidence:\*\* 0.55**  
**\*\*Category:\*\* Network**

Affected Files:

- `azure\_notes.csv`

Locations:

- `azure\_notes.csv`

Evidence:

`

Time,Host,Service,Port,Protocol,Type,Data

2025-09-08 11:50:05

UTC,10.84.185.246,https,443,tcp,nmap.nse.http-stored-xss.tcp.443,{"output"=>"Couldn't find any stored XSS vulnerabilities."}

2025-09-08 11

`

---

### ***VULN-005: Insecure plaintext protocol detected***

**\*\*Severity:\*\* High**  
**\*\*Confidence:\*\* 0.62**  
**\*\*Category:\*\* Transport**

Affected Files:

- `azure\_notes.csv`

Locations:

- `azure\_notes.csv`

Evidence:

`

Time,Host,Service,Port,Protocol,Type,Data

2025-09-08 12:53:46

UTC,10.67.110.154,https,443,tcp,nmap.nse.http-csrf.tcp.443,{"output"=>"Couldn't find any CSRF vulnerabilities."}

2025-09-08 12:53:46 UTC,1

`

---

### ***VULN-006: Weak hash algorithm detected***

**\*\*Severity:\*\* High**  
**\*\*Confidence:\*\* 0.59**  
**\*\*Category:\*\* Crypto**

Affected Files:

- `azure\_notes.csv`

Locations:

- `azure\_notes.csv`

Evidence:

`

Time,Host,Service,Port,Protocol,Type,Data

2025-09-08 12:53:46

UTC,10.67.110.154,https,443,tcp,nmap.nse.http-csrf.tcp.443,{"output"=>"Couldn't find any CSRF vulnerabilities."}

2025-09-08 12:53:46 UTC,1

`

---

### ***VULN-007: Weak encryption algorithm detected***

**\*\*Severity:\*\*** High

**\*\*Confidence:\*\*** 0.62

**\*\*Category:\*\*** Crypto

Affected Files:

• `azure\_notes.csv`

Locations:

• `azure\_notes.csv`

Evidence:

`

Time,Host,Service,Port,Protocol,Type,Data

2025-09-08 12:53:46

UTC,10.67.110.154,https,443,tcp,nmap.nse.http-csrf.tcp.443,{"output"=>"Couldn't find any CSRF vulnerabilities."}

2025-09-08 12:53:46 UTC,1

`

---

### ***VULN-008: Insecure plaintext protocol detected***

**\*\*Severity:\*\*** High

**\*\*Confidence:\*\*** 0.62

**\*\*Category:\*\*** Transport

Affected Files:

• `azure\_notes.csv`

Locations:

• `azure\_notes.csv`

Evidence:

`

Time,Host,Service,Port,Protocol,Type,Data

2025-09-08 13:38:31

UTC,10.80.10.152,https,443,tcp,nmap.nse.http-stored-xss.tcp.443,{"output"=>"Couldn't find any stored XSS vulnerabilities."}

2025-09-08 13:

,  
---

***VULN-009: Insecure plaintext protocol detected***

**\*\*Severity:\*\*** High  
**\*\*Confidence:\*\*** 0.62  
**\*\*Category:\*\*** Transport

Affected Files:

- `azure\_notes.csv`

Locations:

- `azure\_notes.csv`

Evidence:

,

Time,Host,Service,Port,Protocol,Type,Data  
[... truncated ...]

---

***VULN-010: Insecure plaintext protocol detected***

**\*\*Severity:\*\*** High  
**\*\*Confidence:\*\*** 0.62  
**\*\*Category:\*\*** Transport

Affected Files:

- `azure\_services.csv`

Locations:

- `azure\_services.csv`

Evidence:

,

host,port,proto,name,state,info  
10.172.123.57,21,tcp,ftp,filtered,  
10.172.123.57,22,tcp,ssh,filtered,  
10.172.123.57,23,tcp,telnet,filtered,  
10.172.123.57,25,tcp,smtp,filtered,  
10.172.123.57,53,tcp,dns

---

***VULN-011: Insecure plaintext protocol detected***

**\*\*Severity:\*\*** High  
**\*\*Confidence:\*\*** 0.62  
**\*\*Category:\*\*** Transport

Affected Files:

- `azure\_services.csv`

Locations:

- `azure\_services.csv`

Evidence:

`

host,port,proto,name,state,info  
10.172.123.70,21,tcp,ftp,filtered,  
10.172.123.70,22,tcp,ssh,filtered,  
10.172.123.70,23,tcp,telnet,filtered,  
10.172.123.70,25,tcp,smtp,filtered,  
10.172.123.70,53,tcp,dns  
`

---

### ***VULN-012: Insecure plaintext protocol detected***

**\*\*Severity:\*\*** High

**\*\*Confidence:\*\*** 0.62

**\*\*Category:\*\*** Transport

Affected Files:

- `azure\_services.csv`

Locations:

- `azure\_services.csv`

Evidence:

`

host,port,proto,name,state,info  
10.172.123.70,8443,tcp,https-alt,open,Microsoft-HTTPAPI/2.0  
10.172.123.70,8444,tcp,pcsync-http,open,  
10.172.123.70,10001,tcp,scp-config,open,  
10.172.123.70,10002,tcp,do  
`

---

### ***VULN-013: Insecure plaintext protocol detected***

**\*\*Severity:\*\*** High

**\*\*Confidence:\*\*** 0.62

**\*\*Category:\*\*** Transport

Affected Files:

- `azure\_services.csv`

Locations:

- `azure\_services.csv`

Evidence:

`

```
host,port,proto,name,state,info
10.69.72.240,6000,udp,x11,unknown,
10.69.72.240,8080,tcp,http-proxy,filtered,
10.69.72.240,8080,udp,http-alt,unknown,
10.69.72.240,8443,tcp,https-alt,filtered,
10.80.70
```

`

---

### ***VULN-014: Insecure plaintext protocol detected***

**\*\*Severity:\*\*** High  
**\*\*Confidence:\*\*** 0.62  
**\*\*Category:\*\*** Transport

Affected Files:

- `azure\_services.csv`

Locations:

- `azure\_services.csv`

Evidence:

`

```
host,port,proto,name,state,info
10.80.70.36,8080,tcp,http-proxy,filtered,
10.80.70.36,8080,udp,http-alt,unknown,
10.80.70.36,8443,tcp,https-alt,filtered,
10.84.185.246,21,tcp,ftp,filtered,
10.84.185.2
```

`

---

### ***VULN-015: Insecure plaintext protocol detected***

**\*\*Severity:\*\*** High  
**\*\*Confidence:\*\*** 0.62  
**\*\*Category:\*\*** Transport

Affected Files:

- `azure\_services.csv`

Locations:

- `azure\_services.csv`

Evidence:

`

```
host,port,proto,name,state,info
10.84.185.246,8080,udp,http-alt,unknown,
10.84.185.246,8443,tcp,https-alt,filtered,
10.4.64.221,21,tcp,ftp,filtered,
10.4.64.221,22,tcp,ssh,filtered,
10.4.64.221,23,tcp
```

,  
---

### ***VULN-016: Insecure plaintext protocol detected***

**\*\*Severity:\*\*** High  
**\*\*Confidence:\*\*** 0.62  
**\*\*Category:\*\*** Transport

Affected Files:

- `azure\_services.csv`

Locations:

- `azure\_services.csv`

Evidence:

,  
host,port,proto,name,state,info  
10.4.64.221,8080,udp,http-alt,unknown,  
10.4.64.221,8081,tcp,blackice-icecap,open,  
10.4.64.221,8082,tcp,blackice-alerts,open,  
10.4.64.221,8443,tcp,https-alt,open,  
10.4.6  
,

---

### ***VULN-017: Insecure plaintext protocol detected***

**\*\*Severity:\*\*** High  
**\*\*Confidence:\*\*** 0.62  
**\*\*Category:\*\*** Transport

Affected Files:

- `azure\_services.csv`

Locations:

- `azure\_services.csv`

Evidence:

,  
host,port,proto,name,state,info  
10.16.249.246,5432,udp,postgresql,unknown,  
10.16.249.246,5900,tcp,vnc,filtered,  
10.16.249.246,5900,udp,rfb,unknown,  
10.16.249.246,6000,udp,x11,unknown,  
10.16.249.246,80  
,

---

### ***VULN-018: Insecure plaintext protocol detected***



**\*\*Severity:\*\* High**  
**\*\*Confidence:\*\* 0.62**  
**\*\*Category:\*\* Transport**

Affected Files:

- `azure\_services.csv`

Locations:

- `azure\_services.csv`

Evidence:

```
\nhost,port,proto,name,state,info\n10.67.108.106,5900,tcp,vnc,filtered,\n10.67.108.106,5900,udp,rfb,unknown,\n10.67.108.106,6000,udp,x11,unknown,\n10.67.108.106,8080,tcp,http-proxy,filtered,\n10.67.108.106,8\n\n\n---
```

### ***VULN-019: Insecure plaintext protocol detected***

**\*\*Severity:\*\* High**  
**\*\*Confidence:\*\* 0.62**  
**\*\*Category:\*\* Transport**

Affected Files:

- `azure\_services.csv`

Locations:

- `azure\_services.csv`

Evidence:

```
\nhost,port,proto,name,state,info\n10.67.110.154,5900,udp,rfb,unknown,\n10.67.110.154,6000,udp,x11,unknown,\n10.67.110.154,8080,tcp,http-proxy,filtered,\n10.67.110.154,8080,udp,http-alt,unknown,\n10.67.110.1\n\n\n---
```

### ***VULN-020: Insecure plaintext protocol detected***

**\*\*Severity:\*\* High**  
**\*\*Confidence:\*\* 0.62**  
**\*\*Category:\*\* Transport**

Affected Files:

- `azure\_services.csv`

Locations:

- `azure\_services.csv`

Evidence:

`

host,port,proto,name,state,info

10.69.32.242,6000,udp,x11,unknown,

10.69.32.242,8080,tcp,http-proxy,filtered,

10.69.32.242,8080,udp,http-alt,unknown,

10.69.32.242,8443,tcp,https-alt,filtered,

10.69.32

`

---

### ***VULN-021: Insecure plaintext protocol detected***

**\*\*Severity:\*\*** High

**\*\*Confidence:\*\*** 0.62

**\*\*Category:\*\*** Transport

Affected Files:

- `azure\_services.csv`

Locations:

- `azure\_services.csv`

Evidence:

`

host,port,proto,name,state,info

10.80.1.254,5900,udp,rfb,unknown,

10.80.1.254,6000,udp,x11,unknown,

10.80.1.254,8080,tcp,http-proxy,filtered,

10.80.1.254,8080,udp,http-alt,unknown,

10.80.1.254,8443,tc

`

---

### ***VULN-022: Insecure plaintext protocol detected***

**\*\*Severity:\*\*** High

**\*\*Confidence:\*\*** 0.62

**\*\*Category:\*\*** Transport

Affected Files:

- `azure\_services.csv`

Locations:

- `azure\_services.csv`

Evidence:

`

host,port,proto,name,state,info

10.80.4.237,6000,udp,x11,unknown,  
10.80.4.237,8080,tcp,http-proxy,filtered,  
10.80.4.237,8080,udp,http-alt,unknown,  
10.80.4.237,8443,tcp,https-alt,filtered,  
10.80.10.152  
,

---

### ***VULN-023: Insecure plaintext protocol detected***

**\*\*Severity:\*\*** High  
**\*\*Confidence:\*\*** 0.62  
**\*\*Category:\*\*** Transport

Affected Files:

• `azure\_services.csv`

Locations:

• `azure\_services.csv`

Evidence:

,

host,port,proto,name,state,info  
10.80.10.152,8080,tcp,http-proxy,filtered,  
10.80.10.152,8080,udp,http-alt,unknown,  
10.80.10.152,8443,tcp,https-alt,filtered,  
10.80.23.183,21,tcp,ftp,closed,  
10.80.23.18  
,

---

### ***VULN-024: Insecure plaintext protocol detected***

**\*\*Severity:\*\*** High  
**\*\*Confidence:\*\*** 0.62  
**\*\*Category:\*\*** Transport

Affected Files:

• `azure\_services.csv`

Locations:

• `azure\_services.csv`

Evidence:

,

host,port,proto,name,state,info  
10.80.23.183,8080,tcp,http-proxy,filtered,  
10.80.23.183,8080,udp,http-alt,unknown,  
10.80.23.183,8443,tcp,https-alt,filtered,  
10.97.119.225,21,tcp,ftp,filtered,  
10.97.11  
,

---

***VULN-025: Insecure plaintext protocol detected***

**\*\*Severity:\*\*** High

**\*\*Confidence:\*\*** 0.62

**\*\*Category:\*\*** Transport

Affected Files:

- `azure\_services.csv`

Locations:

- `azure\_services.csv`

Evidence:

`

host,port,proto,name,state,info

10.97.119.225,8080,udp,http-alt,unknown,

10.97.119.225,8443,tcp,https-alt,filtered,

10.102.237.149,21,tcp,ftp,filtered,

10.102.237.149,22,tcp,ssh,filtered,

10.102.237.1

`

---

***VULN-026: Insecure plaintext protocol detected***

**\*\*Severity:\*\*** High

**\*\*Confidence:\*\*** 0.62

**\*\*Category:\*\*** Transport

Affected Files:

- `azure\_services.csv`

Locations:

- `azure\_services.csv`

Evidence:

`

host,port,proto,name,state,info

10.102.237.149,8443,tcp,https-alt,filtered,

10.74.240.44,21,tcp,ftp,filtered,

10.74.240.44,22,tcp,ssh,filtered,

10.74.240.44,23,tcp,telnet,filtered,

10.74.240.44,25,tcp

`

---

***VULN-027: Insecure plaintext protocol detected***

**\*\*Severity:\*\*** High

**\*\*Confidence:\*\* 0.62**

**\*\*Category:\*\* Transport**

Affected Files:

- `azure\_services.csv`

Locations:

- `azure\_services.csv`

Evidence:

`

host,port,proto,name,state,info

10.74.240.44,8082,tcp,blackice-alerts,open,

10.74.240.44,8443,tcp,https-alt,open,

10.74.240.44,8444,tcp,pcsync-http,open,

10.74.240.44,10001,tcp,scp-config,open,

10.74.

`

---

### ***VULN-028: Insecure plaintext protocol detected***

**\*\*Severity:\*\* High**

**\*\*Confidence:\*\* 0.62**

**\*\*Category:\*\* Transport**

Affected Files:

- `azure\_services.csv`

Locations:

- `azure\_services.csv`

Evidence:

`

host,port,proto,name,state,info

10.84.194.43,3779,tcp,cognima,closed,

10.84.194.43,3780,tcp,nnp,closed,

10.84.194.43,5432,udp,postgresql,unknown,

10.84.194.43,5900,tcp,vnc,filtered,

10.84.194.43,5900,

`

---

### ***VULN-029: Insecure plaintext protocol detected***

**\*\*Severity:\*\* High**

**\*\*Confidence:\*\* 0.62**

**\*\*Category:\*\* Transport**

Affected Files:

- `azure\_services.csv`

Locations:

- `azure\_services.csv`

Evidence:

`

host,port,proto,name,state,info  
10.91.218.78,3306,tcp,mysql,filtered,  
10.91.218.78,3389,tcp,ms-wbt-server,filtered,  
10.91.218.78,5432,udp,postgresql,unknown,  
10.91.218.78,5900,tcp,vnc,filtered,  
10.91.

`

---

### ***VULN-030: Insecure plaintext protocol detected***

**\*\*Severity:\*\*** High

**\*\*Confidence:\*\*** 0.62

**\*\*Category:\*\*** Transport

Affected Files:

- `azure\_services.csv`

Locations:

- `azure\_services.csv`

Evidence:

`

host,port,proto,name,state,info  
10.105.251.104,636,udp,ldaps,unknown,  
10.105.251.104,993,tcp,imaps,filtered,  
10.105.251.104,995,tcp,pop3s,filtered,  
10.105.251.104,1433,udp,ms-sql-s,unknown,  
10.105.251

`

---

### ***VULN-031: Insecure plaintext protocol detected***

**\*\*Severity:\*\*** High

**\*\*Confidence:\*\*** 0.62

**\*\*Category:\*\*** Transport

Affected Files:

- `azure\_services.csv`

Locations:

- `azure\_services.csv`

Evidence:

`

host,port,proto,name,state,info  
10.159.6.144,993,tcp,imaps,filtered,

10.159.6.144,995,tcp,pop3s,filtered,  
10.159.6.144,1433,udp,ms-sql-s,unknown,  
10.159.6.144,1521,udp,ncube-lm,unknown,  
10.159.6.144,1  
,

---

### ***VULN-032: Insecure plaintext protocol detected***

**\*\*Severity:\*\*** High  
**\*\*Confidence:\*\*** 0.62  
**\*\*Category:\*\*** Transport

Affected Files:

• `azure\_services.csv`

Locations:

• `azure\_services.csv`

Evidence:

,

host,port,proto,name,state,info  
10.161.154.129,993,tcp,imaps,filtered,  
10.161.154.129,995,tcp,pop3s,filtered,  
10.161.154.129,1433,udp,ms-sql-s,unknown,  
10.161.154.129,1521,udp,ncube-lm,unknown,  
10.161  
,

---

### ***VULN-033: Insecure plaintext protocol detected***

**\*\*Severity:\*\*** High  
**\*\*Confidence:\*\*** 0.62  
**\*\*Category:\*\*** Transport

Affected Files:

• `azure\_services.csv`

Locations:

• `azure\_services.csv`

Evidence:

,

host,port,proto,name,state,info  
10.162.198.248,995,tcp,pop3s,filtered,  
10.162.198.248,1433,udp,ms-sql-s,unknown,  
10.162.198.248,1521,udp,ncube-lm,unknown,  
10.162.198.248,1723,tcp,pptp,filtered,  
10.162  
,

---

### ***VULN-034: Insecure plaintext protocol detected***

**\*\*Severity:\*\*** High

**\*\*Confidence:\*\*** 0.62

**\*\*Category:\*\*** Transport

Affected Files:

- `azure\_services.csv`

Locations:

- `azure\_services.csv`

Evidence:

`

host,port,proto,name,state,info

10.162.251.64,1433,udp,ms-sql-s,unknown,

10.162.251.64,1521,udp,ncube-lm,unknown,

10.162.251.64,1723,tcp,pptp,filtered,

10.162.251.64,3306,tcp,mysql,filtered,

10.162.25

`

---

### ***VULN-035: Insecure plaintext protocol detected***

**\*\*Severity:\*\*** High

**\*\*Confidence:\*\*** 0.62

**\*\*Category:\*\*** Transport

Affected Files:

- `azure\_services.csv`

Locations:

- `azure\_services.csv`

Evidence:

`

host,port,proto,name,state,info

10.237.31.167,1521,udp,ncube-lm,unknown,

10.237.31.167,1723,tcp,pptp,filtered,

10.237.31.167,3306,tcp,mysql,filtered,

10.237.31.167,3389,tcp,ms-wbt-server,filtered,

10.

`

---

### ***VULN-036: Insecure plaintext protocol detected***

**\*\*Severity:\*\*** High



**\*\*Confidence:\*\*** 0.62

**\*\*Category:\*\*** Transport

Affected Files:

• `azure\_services.csv`

Locations:

• `azure\_services.csv`

Evidence:

`

host,port,proto,name,state,info

10.252.176.154,1723,tcp,pptp,filtered,

10.252.176.154,3306,tcp,mysql,filtered,

10.252.176.154,3389,tcp,ms-wbt-server,filtered,

10.252.176.154,5432,udp,postgresql,unknown

`

---

### ***VULN-037: Insecure plaintext protocol detected***

**\*\*Severity:\*\*** High

**\*\*Confidence:\*\*** 0.62

**\*\*Category:\*\*** Transport

Affected Files:

• `azure\_services.csv`

Locations:

• `azure\_services.csv`

Evidence:

`

host,port,proto,name,state,info

10.47.159.57,3306,tcp,mysql,filtered,

10.47.159.57,3389,tcp,ms-wbt-server,filtered,

10.47.159.57,5432,udp,postgresql,unknown,

10.47.159.57,5900,tcp,vnc,filtered,

10.47.

`

---

### ***VULN-038: Insecure plaintext protocol detected***

**\*\*Severity:\*\*** High

**\*\*Confidence:\*\*** 0.62

**\*\*Category:\*\*** Transport

Affected Files:

• `azure\_services.csv`

Locations:

• `azure\_services.csv`

Evidence:

`

host,port,proto,name,state,info  
10.210.211.63,3389,tcp,ms-wbt-server,filtered,  
10.210.211.63,5432,udp,postgresql,unknown,  
10.210.211.63,5900,tcp,vnc,filtered,  
10.210.211.63,5900,udp,rfb,unknown,  
10.21

`

---

### ***VULN-039: Insecure plaintext protocol detected***

**\*\*Severity:\*\*** High

**\*\*Confidence:\*\*** 0.62

**\*\*Category:\*\*** Transport

Affected Files:

• `azure\_services.csv`

Locations:

• `azure\_services.csv`

Evidence:

`

host,port,proto,name,state,info  
10.214.27.37,5432,udp,postgresql,unknown,  
10.214.27.37,5900,tcp,vnc,filtered,  
10.214.27.37,5900,udp,rfb,unknown,  
10.214.27.37,6000,udp,x11,unknown,  
10.214.27.37,8080,tc

`

---

### ***VULN-040: Insecure plaintext protocol detected***

**\*\*Severity:\*\*** High

**\*\*Confidence:\*\*** 0.62

**\*\*Category:\*\*** Transport

Affected Files:

• `azure\_services.csv`

Locations:

• `azure\_services.csv`

Evidence:

`

host,port,proto,name,state,info  
10.183.61.130,5900,tcp,vnc,filtered,  
10.183.61.130,5900,udp,rfb,unknown,

10.183.61.130,6000,udp,x11,unknown,  
10.183.61.130,8080,tcp,http-proxy,filtered,  
10.183.61.130,8  
,

---

### ***VULN-041: Insecure plaintext protocol detected***

**\*\*Severity:\*\*** High  
**\*\*Confidence:\*\*** 0.62  
**\*\*Category:\*\*** Transport

Affected Files:

- `on-prem\_services.csv`

Locations:

- `on-prem\_services.csv`

Evidence:

,  
host,port,proto,name,state,info  
10.90.242.1,21,tcp,ftp,closed,  
10.90.242.1,22,tcp,ssh,closed,  
10.90.242.1,23,tcp,telnet,closed,  
10.90.242.1,25,tcp,smtp,filtered,  
10.90.242.1,53,tcp,domain,closed,  
10.9  
,

---

### ***VULN-042: Insecure plaintext protocol detected***

**\*\*Severity:\*\*** High  
**\*\*Confidence:\*\*** 0.62  
**\*\*Category:\*\*** Transport

Affected Files:

- `on-prem\_services.csv`

Locations:

- `on-prem\_services.csv`

Evidence:

,  
host,port,proto,name,state,info  
10.90.242.1,5900,udp,rfb,filtered,  
10.90.242.1,6000,udp,x11,filtered,  
10.90.242.1,8080,tcp,http-proxy,closed,  
10.90.242.1,8080,udp,http-alt,unknown,  
10.90.242.1,8443,tc  
,

---

### ***VULN-043: Insecure plaintext protocol detected***

**\*\*Severity:\*\*** High

**\*\*Confidence:\*\*** 0.62

**\*\*Category:\*\*** Transport

Affected Files:

- `on-prem\_services.csv`

Locations:

- `on-prem\_services.csv`

Evidence:

`

host,port,proto,name,state,info

10.90.242.12,5900,tcp,vnc,filtered,

10.90.242.12,5900,udp,rfb,unknown,

10.90.242.12,6000,udp,x11,unknown,

10.90.242.12,8080,tcp,http-proxy,filtered,

10.90.242.12,8080,u

`

---

### ***VULN-044: Insecure plaintext protocol detected***

**\*\*Severity:\*\*** High

**\*\*Confidence:\*\*** 0.62

**\*\*Category:\*\*** Transport

Affected Files:

- `on-prem\_services.csv`

Locations:

- `on-prem\_services.csv`

Evidence:

`

host,port,proto,name,state,info

10.90.242.25,5432,udp,postgresql,unknown,

10.90.242.25,5900,tcp,vnc,filtered,

10.90.242.25,5900,udp,rfb,unknown,

10.90.242.25,6000,udp,x11,unknown,

10.90.242.25,8080,tc

`

---

### ***VULN-045: Insecure plaintext protocol detected***

**\*\*Severity:\*\*** High

**\*\*Confidence:\*\* 0.62**

**\*\*Category:\*\* Transport**

Affected Files:

• `on-prem\_services.csv`

Locations:

• `on-prem\_services.csv`

Evidence:

```
host,port,proto,name,state,info
10.90.242.27,5900,tcp,vnc,filtered,
10.90.242.27,5900,udp,rfb,closed,
10.90.242.27,6000,udp,x11,closed,
10.90.242.27,8080,tcp,http-proxy,filtered,
10.90.242.27,8080,udp
```

---

### ***VULN-046: Insecure plaintext protocol detected***

**\*\*Severity:\*\* High**

**\*\*Confidence:\*\* 0.62**

**\*\*Category:\*\* Transport**

Affected Files:

• `on-prem\_services.csv`

Locations:

• `on-prem\_services.csv`

Evidence:

```
host,port,proto,name,state,info
10.90.242.34,5432,udp,postgresql,unknown,
10.90.242.34,5900,tcp,vnc,filtered,
10.90.242.34,5900,udp,rfb,unknown,
10.90.242.34,6000,udp,x11,unknown,
10.90.242.34,8080,tc
```

---

## **Risk Overview**

Risk Overview

=====

Total Active Findings: 46

High Severity (44 findings):

Requires immediate attention. These findings pose significant security risks

and should be remediated as a priority.

Medium Severity (2 findings):

Should be addressed in the near term. These findings indicate potential security concerns that should be evaluated in context.

Low Severity (0 findings):

May be addressed as resources permit. These findings represent lower-risk issues or hygiene improvements.