

# ESL Pro Security Report

Generated on: 2025-09-11 15:18:36 ADT

## Executive Summary

The security scan revealed a moderate risk level, primarily driven by the detection of several processes without digital signatures and unusual locations of system processes. While no critical vulnerabilities were identified, the presence of unsigned executables and atypical process behavior warrants immediate investigation and further security measures to mitigate potential threats.

## Antivirus Status

{'C:\\Windows\\Temp': '', 'C:\\Users\\leaw0\\Downloads': ''}

## Firewall Status

Domain Profile Settings: ----- State ON Firewall  
Policy BlockInbound,AllowOutbound LocalFirewallRules N/A (GPO-store only) LocalConSecRules  
N/A (GPO-store only) InboundUserNotification Enable RemoteManagement Disable  
UnicastResponseToMulticast Enable Logging: LogAllowedConnections Disable  
LogDroppedConnections Disable FileName %systemroot%\system32\LogFiles\Firewall\pfirewall.log  
MaxFileSize 4096 Private Profile Settings: -----  
State ON Firewall Policy BlockInbound,AllowOutbound LocalFirewallRules N/A (GPO-store only)  
LocalConSecRules N/... [truncated]

## Network Status

{'nmap': {'command\_line': 'nmap -oX - -sV 127.0.0.1', 'scaninfo': {'tcp': {'method': 'syn', 'services':  
'1,3-4,6-7,9,13,17,19-26,30,32-33,37,42-43,49,53,70,79-85,88-90,99-100,106,109-1  
11,113,119,125,135,139,143-144,146,161,163,179,199,211-212,222,254-256,259,264,2  
80,301,306,311,340,366,389,406-407,416-417,425,427,443-445,458,464-465,481,497,5

00,512-515,524,541,543-545,548,554-555,563,587,593,616-617,625,631,636,646,648,6  
66-668,683,687,691,700,705,711,714,720,722,726,749,765,777,783,787,800-801,808,8  
43,873,880,888,898,900-903,911-912,981,987,990,992-993,995,999-1002,1007,1009-10  
11,1021-1100,1102,1104-1108,1110-1114,1117,1119,1121-1124,1126,1130-1132,1137-11  
38,1141,1145,1147-1149,1151-1152,1154,1163-1166,1169,1174-1175,1183,1185-1187,11  
92,1198-1199,1201,1213,1216-1218,1233-1234,1236,1244,1247-1248,1259,1271-1272,12  
77,1287,1296,1300-1301,1309-1311,1322,1328,1334,1352,1417,1433-1434,1443,1455,14  
61,1494,1500-1501,1503,1521,1524,1533,1556,1580,1583,1594,1600,1641,1658,1666,16  
87-1688,1700,171... [truncated]

## Process Security

```
{'scan_time': '2025-09-11T15:17:52.361792', 'total_processes': 279, 'suspicious_processes': 5,  
'high_resource_processes': 0, 'network_processes': 43, 'processes': [{'pid': 272, 'name': 'Registry',  
'exe_path': 'Registry', 'cmdline': '', 'cpu_percent': 0.0, 'memory_percent': 0.04978010724313682,  
'create_time': '2025-09-10T16:43:08.567507', 'username': None, 'status': 'running', 'num_threads': 4,  
'network_connections': 0, 'listening_ports': []}, {'pid': 848, 'name': 'smss.exe', 'exe_path':  
'C:\\\\Windows\\System32\\smss.exe', 'cmdline': '', 'cpu_percent': 0.0, 'memory_percent':  
0.0020373915261975863, 'create_time': '2025-09-10T16:43:11.156373', 'username': None, 'status':  
'running', 'num_threads': 2, 'network_connections': 0, 'listening_ports': [], 'file_size': 228768,  
'file_modified': '2025-09-10T14:48:49.654519', 'file_created': '2025-09-10T14:48:49.633183',  
'file_hash_partial': 'e63a0ddb7bd59f22fb5c2ad66e65d61b', 'digitally_signed': True}, {'pid': 936,  
'name': 'svchost.exe', 'exe_path': ... [truncated]}
```

# Vulnerability Scan Results

[OK] No vulnerabilities detected in the scanned directories.

## OSV Scanner Details

[DATA] Total 6 packages affected by 27 known vulnerabilities (2 Critical, 10 High, 11 Medium, 2 Low, 2 Unknown) from 1 ecosystem.

[SCA]  
Medi

## Network Traffic Analysis

Analyzed 21 network connections

## Process Security Analysis

Scanned 279 processes, found 5 suspicious processes. Process security risk level: MEDIUM

### Key Process Findings:

Found 5 potentially suspicious processes

Susp

# AI Security Recommendations

## Detailed Analysis & Recommendations

1. **\*\*Investigate Unsigned Processes Immediately:\*\*** Prioritize investigating the processes identified as lacking digital signatures (LibreViewMASMonitor.exe, WidgetService.exe, and explorer.exe). Use process explorer or task manager to examine the processes activities, network connections, and parent processes. If any suspicious activity is observed, isolate the process and consider a full malware scan.

2. **\*\*Verify System Process Locations:\*\*** Confirm that all system processes (like explorer.exe) are running from their standard, protected locations. A change in location is a strong signal of a compromised system or malicious software attempting to masquerade as a legitimate process.

3. **\*\*Run a Full Antivirus Scan:\*\*** Conduct a thorough antivirus scan across the entire system, specifically targeting the identified suspicious processes and their associated files. Use a reputable antivirus solution that offers real-time scanning and protection.

4. **\*\*Implement Process Monitoring and Alerting:\*\*** Configure a system for monitoring process activity. Set up alerts to notify administrators when unusual processes are launched or when processes deviate from their expected behavior. This proactive monitoring can help detect and respond to threats quickly.

5. **\*\*Regularly Update Software and OS:\*\*** Ensure all software, including the operating system and applications, are kept up to date with the latest security patches. Outdated software is a common entry point for attackers. ---

## Risk Assessment

Overall Risk Level: LOW - System appears secure