

ESL Pro Security Report

Generated on: 2025-09-14 18:07:01 ADT

Executive Summary

This security analysis reveals a medium risk level due to the presence of five potentially suspicious processes and one process lacking a digital signature. While no critical vulnerabilities were detected, the unusual execution of `explorer.exe` and the lack of digital signature on `LibreViewMASMonitor.exe` warrant immediate investigation and proactive security measures.

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': '2025-09-14T18:07:01.226575', 'total_processes': 248, 'suspicious_processes': 5,
'high_resource_processes': 0, 'network_processes': 36, 'processes': [{'pid': 272, 'name': 'Registry',
'exe_path': 'Registry', 'cmdline': '', 'cpu_percent': 0.0, 'memory_percent': 0.0805700077549706,
'create_time': '2025-09-14T11:10:53.581732', 'username': None, 'status': 'running', 'num_threads': 4,
'network_connections': 0, 'listening_ports': []}, {'pid': 368, 'name': 'ApplicationFrameHost.exe',
'exe_path': 'C:\\Windows\\System32\\ApplicationFrameHost.exe', 'cmdline':
'C:\\WINDOWS\\system32\\ApplicationFrameHost.exe -Embedding', 'cpu_percent': 0.0,
'memory_percent': 0.07215801417022506, 'create_time': '2025-09-14T11:18:17.099874',
'username': 'DESKTOP-DUQ7M23\\leaw0', 'status': 'running', 'num_threads': 33,
'network_connections': 0, 'listening_ports': [], 'file_size': 96504, 'file_modified':
'2025-04-25T18:10:17.261243', 'file_created': '2025-04-25T18:10:17.250240', 'file_hash_partial':
'435... [truncated]}
```

Vulnerability Scan Results

[OK] No vulnerabilities detected in the scanned directories.

OSV Scanner Details

OSV Results: No output from scanner

Network Traffic Analysis

Analyzed 30 network connections

Process Security Analysis

Scanned 248 processes, found 5 suspicious processes. Process security risk level: MEDIUM

Key Process Findings:

Found 5 potentially suspicious processes

Susp
c:\win

AI Security Recommendations

Detailed Analysis & Recommendations

1. ****Immediate Investigation of Suspicious Processes:**** Prioritize investigating the processes identified as suspicious - `explorer.exe` (PID: 9260) and `LibreViewMASMonitor.exe` (PID: 10144). Use process monitoring tools to understand their behavior, network connections, and resource usage. 2. ****Digital Signature Verification:**** Ensure all executable files, particularly those from third-party software, are digitally signed by a trusted vendor. Investigate why `LibreViewMASMonitor.exe` lacks a digital signature and determine if it's a legitimate absence or a potential security risk. 3. ****Enhanced Process Monitoring & Alerting:**** Implement or optimize existing process monitoring solutions to actively track resource usage, network activity, and command-line arguments of potentially risky processes. Set up alerts for anomalous behavior, such as unexpected network connections or elevated privileges. 4. ****Full Antivirus Scan:**** Conduct a comprehensive full system scan using a reputable antivirus solution to identify and remove any malware or suspicious files. 5. ****Regular Security Audits & Process Reviews:**** Establish a schedule for regular security audits, including reviewing running processes, executable files, and security configurations, to identify and address potential vulnerabilities proactively.

Risk Assessment

Overall Risk Level: LOW - System appears secure