ESL Pro Security Report

Generated on: 2025-09-16 15:31:42 ADT

Executive Summary

The system exhibits a medium risk level due to the detection of several processes lacking digital signatures and one running from an unusual location. While no critical vulnerabilities were identified, the presence of unsigned executables and unusual process locations warrants immediate investigation to prevent potential compromise. Further proactive security measures, including regular scanning and process monitoring, are recommended.

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': '2025-09-16T15:31:42.628090', 'total_processes': 258, 'suspicious_processes': 4, 'high_resource_processes': 0, 'network_processes': 38, 'processes': [{'pid': 272, 'name': 'Registry', 'exe_path': 'Registry', 'cmdline': '', 'cpu_percent': 0.0, 'memory_percent': 0.05296263686368433, 'create_time': '2025-09-15T14:30:04.581497', 'username': None, 'status': 'running', 'num_threads': 4, 'network_connections': 0, 'listening_ports': []}, {'pid': 472, 'name': 'pwsh.exe', 'exe_path': 'C:\\Program Files\\PowerShell\\7\\pwsh.exe', 'cmdline': 'C:\\Program Files\\PowerShell\\7\\pwsh.exe -noexit -command try { . "c:\\Users\\leaw0\\AppData\\Local\\Programs\\Microsoft VS Code\\resources\\app\\out\\vs\\workbench\\contrib\\terminal\\common\\scripts\\sh ellIntegration.ps1" } catch {}', 'cpu_percent': 0.0, 'memory_percent': 0.13296484698020644, 'create_time': '2025-09-15T16:57:43.580479', 'username': 'DESKTOP-DUQ7M23\\leaw0', 'status': 'running', 'num_threads': 16, 'network_connections': 0, 'li... [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 26 network connections

Process Security Analysis

Scanned 258 processes, found 4 suspicious processes. Process security risk level: MEDIUM

Key Process Findings:

Found 4 potentially suspicious processes

Susp

AI Security Recommendations

Detailed Analysis & Recommendations

1. **Investigate Unsigned Processes Immediately:** Prioritize immediate investigation into the executables: `Video.UI.exe (PID: 3720)` and `explorer.exe (PID: 9420)`. Use tools like Process Explorer or Sysinternals Suite to analyze these processes, including their parent processes, network connections, and loaded modules. Determine why they are running without digital signatures - is it a legitimate but un-signed application, or something more sinister? 2. **Implement Digital Signature Verification:** Strengthen security controls to ensure all system processes, especially those running from unexpected locations, are digitally signed by trusted publishers. This will help prevent the execution of malicious code. 3. **Enhance Process Monitoring and Alerting:** Configure enhanced process monitoring to detect and alert on unexpected process behavior, such as processes running from unusual locations, spawning new processes, or establishing network connections. Sysmon is a great tool for this. 4. **Regular Security Audits and Process Reviews**: Implement a scheduled audit to check for new suspicious process or system process changes, as well as ensure that the system configuration remains secure. 5. **Update Antivirus/Anti-Malware Software:** Ensure that antivirus/anti-malware software is up-to-date with the latest definitions and signatures. Run a full system scan to check for any malware infections. **Important Note:** This analysis is based solely on the provided data. A comprehensive security assessment would require a deeper dive into system logs, network traffic, and other security information.

Risk Assessment

Overall Risk Level: LOW - System appears secure