ESL Pro Security Report

Generated on: 2025-09-14 00:13:19 ADT

Executive Summary

The system exhibits a HIGH overall security risk level due to the detection of several potentially suspicious processes and the absence of digital signatures on key executable files like WidgetService.exe and explorer.exe. Further investigation and remediation are required to mitigate these vulnerabilities and strengthen the systems security posture. The presence of multiple active network connections and a large number of processes also contribute to the elevated risk.

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': '2025-09-14T00:12:43.234455', 'total_processes': 289, 'suspicious_processes': 6, 'high_resource_processes': 0, 'network_processes': 41, 'processes': [{'pid': 272, 'name': 'Registry', 'exe_path': 'Registry', 'cmdline': '', 'cpu_percent': 0.0, 'memory_percent': 0.06806891689165052, 'create_time': '2025-09-13T22:22:19.566424', 'username': None, 'status': 'running', 'num_threads': 4, 'network_connections': 0, 'listening_ports': []}, {'pid': 760, 'name': 'steamwebhelper.exe', 'exe_path': 'C:\\Program Files (x86)\\Steam\\bin\\cef\\cef.win7x64\\steamwebhelper.exe', 'cmdline': 'C:\\Program Files (x86)\\Steam\\bin\\cef\\cef.win7x64\\steamwebhelper.exe --type=renderer --user-agent-product=Valve Steam Client --user-data-dir=C:\\Users\\leaw0\\AppData\\Local\\Steam\\htmlcache --buildid=1757452101 --steamid=0 --valve-initial-threadpool-size=4 --lang=en-GB --device-scale-factor=1 --num-raster-threads=4 --enable-main-frame-before-activation --renderer-client-id=5 --time-ticks-at-unix-epo... [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 29 network connections

Process Security Analysis

Scanned 289 processes, found 6 suspicious processes. Process security risk level: HIGH

Key Process Findings:

Found 6 potentially suspicious processes

Susp
c:\wir

AI Security Recommendations

Detailed Analysis & Recommendations

1. **Immediate Investigation of Suspicious Processes:** Prioritize investigating the processes identified as suspicious (explorer.exe, WidgetService.exe, and LibreViewMASMonitor.exe) immediately. Utilize tools to determine their legitimate purpose and origin. 2. **Digital Signature Verification and Remediation:** Verify the legitimacy of all executable files, particularly those that are not digitally signed. If unsigned executables are found, determine their source and address the root cause of the lack of digital signatures. Contact the developers to ensure proper signing. 3. **Enhanced Process Monitoring and Alerting:** Implement or strengthen process monitoring and alerting systems to promptly identify and flag any unusual process behavior. This includes setting up alerts for processes running from non-standard locations, excessive resource consumption, or connections to suspicious network locations. 4. **Run Full Antivirus Scan:** Execute a full system scan using a reputable antivirus solution to detect and remove any malware or malicious software. Ensure antivirus definitions are up-to-date. 5. **Review Network Connections:** Analyze all active network connections to identify any unauthorized or suspicious connections. Implement stricter firewall rules to block any connections to known malicious domains or IPs.

Risk Assessment

Overall Risk Level: LOW - System appears secure