ESL Pro Security Report

Generated on: 2025-09-17 15:19:46 ADT

Executive Summary

The system exhibits a medium security risk level due to the presence of several processes without digital signatures and unusual process locations. While the antivirus and firewall are active, the system's processes present potential vulnerabilities that require immediate investigation. Further security measures, including regular audits and process monitoring, are recommended to mitigate these risks.

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': '1,3-4,6-7,9,13,17,19-26,30,32-33,37,42-43,49,53,70,79-85,88-90,99-100,106,109-111,113,119,125,135,139,143-144,146,161,163,179,199,211-212,222,254-256,259,264,2

80,301,306,311,340,366,389,406-407,416-417,425,427,443-445,458,464-465,481,497,500,512-515,524,541,543-545,548,554-555,563,587,593,616-617,625,631,636,646,648,666-668,683,687,691,700,705,711,714,720,722,726,749,765,777,783,787,800-801,808,843,873,880,888,898,900-903,911-912,981,987,990,992-993,995,999-1002,1007,1009-1011,1021-1100,1102,1104-1108,1110-1114,1117,1119,1121-1124,1126,1130-1132,1137-1138,1141,1145,1147-1149,1151-1152,1154,1163-1166,1169,1174-1175,1183,1185-1187,1192,1198-1199,1201,1213,1216-1218,1233-1234,1236,1244,1247-1248,1259,1271-1272,1277,1287,1296,1300-1301,1309-1311,1322,1328,1334,1352,1417,1433-1434,1443,1455,1461,1494,1500-1501,1503,1521,1524,1533,1556,1580,1583,1594,1600,1641,1658,1666,1687-1688,1700,171... [truncated]

Process Security

{'scan_time': '2025-09-17T15:19:26.698422', 'total_processes': 281, 'suspicious_processes': 5, 'high_resource_processes': 0, 'network_processes': 40, 'processes': [{'pid': 272, 'name': 'Registry', 'exe_path': 'Registry', 'cmdline': '', 'cpu_percent': 0.0, 'memory_percent': 0.03833349770836396, 'create_time': '2025-09-17T09:47:29.565886', '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': 0.002099419839641541, 'create_time': '2025-09-17T09:47:32.274191', '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': 1072, 'name': 'csrss.exe', 'exe_path': 'C... [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 20 network connections

Process Security Analysis

Scanned 281 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 and Remove Non-Digitally Signed Processes:** Immediately investigate notepad++.exe (PID: 1408) and WidgetService.exe (PID: 13760) - these processes lack digital signatures, indicating a potential for malicious code. Determine their purpose and remove if unnecessary or if they originate from untrusted sources. 2. **Monitor System Process Locations:** Implement stricter controls around the execution of system processes, such as explorer.exe. Verify that explorer.exe is running from the standard Windows directory (C:\Windows\explorer.exe) and investigate any instances running from unusual locations - as detected. Implement process sandboxing and monitoring for deviations. 3. **Enable Digital Signature Verification:** Ensure that Windows Defender or a comparable security solution is configured to enforce digital signature verification for all executable files. This will prevent the execution of untrusted software. 4. **Implement Enhanced Process Monitoring:** Utilize system monitoring tools to track process activity in real-time. Set alerts for unexpected process execution, high resource usage, or unusual network connections. This allows for rapid detection and response to potential threats. 5. **Regular Security Audits:** Schedule regular security audits to review system configurations, process execution, and network activity. This proactive approach helps identify and address vulnerabilities before they can be exploited.

Risk Assessment

Overall Risk Level: LOW - System appears secure