ESL Pro Security Report

Generated on: 2025-09-23 11:50:44 ADT

Executive Summary

This security scan revealed a medium risk level due to the presence of five potentially suspicious processes and unusual execution locations for system processes. While the antivirus and firewall are active, the scan identified instances where system processes are running from non-standard locations, warranting immediate investigation. Further monitoring and strengthening of security protocols are recommended 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': '2025-09-23T11:49:06.404339', 'total_processes': 252, 'suspicious_processes': 5, 'high_resource_processes': 0, 'network_processes': 37, 'processes': [{'pid': 272, 'name': 'Registry', 'exe_path': 'Registry', 'cmdline': '', 'cpu_percent': 0.0, 'memory_percent': 0.04831051335538774, 'create_time': '2025-09-23T11:25:15.566421', 'username': None, 'status': 'running', 'num_threads': 4, 'network_connections': 0, 'listening_ports': []}, {'pid': 860, 'name': 'Code.exe', 'exe_path': 'C:\\Users\\leaw0\\AppData\\Local\\Programs\\Microsoft VS Code\\Code.exe', 'cmdline': 'C:\\Users\\leaw0\\AppData\\Local\\Programs\\Microsoft VS Code\\Code.exe c:\\Users\\leaw0\\.vscode\\extensions\\ms-python.vscode-pylance-2025.8.2\\dist\\ server.bundle.js --cancellationReceive=file:4277636da3349367c7120a42de07db61e33293a7d7 --node-ipc --clientProcessId=16624', 'cpu_percent': 0.0, 'memory_percent': 0.4992754377278437, 'create_time': '2025-09-23T11:26:41.367391', 'username': 'DESKTOP-DUQ7M23\\leaw0', 'sta... [truncated]

Vulnerability Scan Results

Vulnerability Summary

Total Vulnerabilities Found: 40

Vulnerabilities by Package:

aiohttp: 17 vulnerabilities (HIGH PRIORITY)

flask: 2 vulnerabilities (LOW PRIORITY)

lxml: 2 vulnerabilities (LOW PRIORITY)

requests: 4 vulnerabilities (MEDIUM PRIORITY)

torch: 10 vulnerabilities (HIGH PRIORITY)

werkzeug: 5 vulnerabilities (MEDIUM PRIORITY)

OSV Scanner Details

Network Traffic Analysis

Analyzed 2 network connections

Process Security Analysis

Scanned 252 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 Suspicious Processes Immediately:** Prioritize investigation of the five identified processes (notepad++.exe, explorer.exe, WidgetService.exe, and other suspicious processes). Use process monitoring tools to track their activities, network connections, and file system access. 2. **Verify System Process Locations:** Confirm that explorer.exe and other system processes are executing from their standard locations within `C:\Windows\System32`. Remediation should involve restoring these processes to their correct locations. 3. **Run Full Antivirus Scan:** Conduct a comprehensive full system scan using a reputable antivirus solution to detect and remove any malware or malicious software associated with the identified suspicious processes. 4. **Implement Process Monitoring and Alerting:** Deploy or enhance existing process monitoring tools to provide real-time alerts for unusual process behavior, network connections, and file system modifications. This allows for rapid response to potential threats. 5. **Review Network Connections:** Analyze network connections originating from the identified processes. Identify any unauthorized communication and implement appropriate firewall rules or network segmentation to restrict access. --- **Note:** This analysis is based solely on the provided scan results. A complete security assessment would require more detailed information about the system configuration, user activity, and network environment.

Risk Assessment

Overall Risk Level: MEDIUM - Review and address issues