

ESL Pro Security Report

Generated on: 2025-09-18 22:29:23 ADT

Executive Summary

The system exhibits a HIGH security risk level due to multiple suspicious processes, including one lacking digital signatures and an explorer.exe instance running from an atypical location. Several processes are consuming significant network resources. Immediate investigation and remediation are warranted 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': '2025-09-18T22:29:23.472977', 'total_processes': 262, 'suspicious_processes': 6,  
'high_resource_processes': 0, 'network_processes': 37, 'processes': [{'pid': 272, 'name': 'Registry',  
'exe_path': 'Registry', 'cmdline': '', 'cpu_percent': 0.0, 'memory_percent': 0.07268286913013546,  
'create_time': '2025-09-18T14:02:35.582365', 'username': None, 'status': 'running', 'num_threads': 4,  
'network_connections': 0, 'listening_ports': []}, {'pid': 876, 'name': 'smss.exe', 'exe_path':  
'C:\\\\Windows\\System32\\smss.exe', 'cmdline': '', 'cpu_percent': 0.0, 'memory_percent':  
0.002089877022188625, 'create_time': '2025-09-18T14:02:38.343807', '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': 980,  
'name': 'svchost.exe', 'exe_path': '... [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 8 network connections

Process Security Analysis

Scanned 262 processes, found 6 suspicious processes. Process security risk level: HIGH

Key Process Findings:

Found 6 potentially suspicious processes

Susp

AI Security Recommendations

Detailed Analysis & Recommendations

1. ****Immediate Investigation of Suspicious Processes:**** Prioritize investigating WidgetService.exe (PID: 2420) and explorer.exe (PID: 9628) immediately. Use process monitoring tools to track their activity and verify their legitimacy. Analyze the code of these processes to confirm they are authorized and from legitimate sources.

2. ****Digital Signature Verification:**** Implement stricter policies regarding digitally signed executables. Ensure all system processes and third-party applications are digitally signed by trusted vendors. Enforce scanning of downloaded and installed software to identify unsigned or compromised files.

3. ****Process Isolation & Monitoring:**** Implement robust process monitoring and alerting. Utilize tools to track process behavior, network activity, and resource consumption. Set up alerts for unusual or unexpected process activity, particularly around the identified suspicious processes. Consider isolating potentially risky processes to limit their impact if compromised.

4. ****Review System Configuration:**** Conduct a comprehensive review of the system configuration, including user accounts, permissions, and firewall rules. Ensure that the system adheres to security best practices and that all unnecessary services are disabled.

5. ****Regular Security Audits & Updates:**** Schedule regular security audits to identify and address vulnerabilities. Maintain up-to-date antivirus definitions, operating system patches, and software updates. Implement a robust vulnerability scanning program.

****Note:**** The presence of multiple listening ports also warrants further investigation. Determine the purpose of these ports and ensure they are properly configured and secured.

Risk Assessment

Overall Risk Level: MEDIUM - Review and address issues