A-Ryan Security Report

Generated on: 2025-09-25 22:53:55 ADT

Executive Summary

The system scan revealed a high level of security risk primarily due to the presence of unsigned processes and a significant number of listening ports. While no vulnerabilities were explicitly identified within the scanned processes, the lack of digital signatures and active network connections warrant immediate investigation. This necessitates a focused effort to identify and 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': '2025-09-25T22:52:38.341176', 'total_processes': 268, 'suspicious_processes': 9, 'high_resource_processes': 0, 'network_processes': 36, 'processes': [{'pid': 272, 'name': 'Registry', 'exe_path': 'Registry', 'cmdline': '', 'cpu_percent': 0.0, 'memory_percent': 0.07821770325282679, 'create_time': '2025-09-25T14:42:55.567077', 'username': None, 'status': 'running', 'num_threads': 4, 'network_connections': 0, 'listening_ports': []}, {'pid': 856, 'name': 'svchost.exe', 'exe_path': 'C:\\Windows\\System32\\svchost.exe', 'cmdline': '', 'cpu_percent': 0.0, 'memory_percent': 0.02090354163061271, 'create_time': '2025-09-25T14:43:08.467242', 'username': None, 'status': 'running', 'num_threads': 7, 'network_connections': 2, 'listening_ports': [49666, 49666], 'file_size': 88232, 'file_modified': '2025-09-10T14:48:48.612114', 'file_created': '2025-09-10T14:48:48.593875', 'file_hash_partial': '09d6bb18abb809eee33c5961a1c92b62', 'digitally_signed': True}, {'pid': 884, 'name': 'smss.exe', ... [truncated]

Vulnerability Scan Results

[OK] No vulnerabilities detected in the scanned directories.

OSV Scanner Details

Network Traffic Analysis

Analyzed 3 network connections

Process Security Analysis

Scanned 268 processes, found 9 suspicious processes. Process security risk level: HIGH

Key Process Findings:

Found 9 potentially suspicious processes

Susp

AI Security Recommendations

Detailed Analysis & Recommendations

1. **Investigate Unsigned Processes Immediately:** Prioritize investigating all 9 processes flagged as not digitally signed. Determine the origin and purpose of each, and confirm their legitimacy. The lack of digital signatures is a major red flag and likely indicates malware or unauthorized software. 2. **Review Network Listening Ports:** Thoroughly audit the systems network listening ports (currently 22). Determine the purpose of each port and ensure they are legitimately required. Unnecessary ports represent potential entry points for attackers. Disable any ports not actively used. 3. **Implement Digital Signature Verification:** Enforce a policy requiring all executable files to be digitally signed by trusted Certificate Authorities. This will significantly reduce the risk of malware execution. 4. **Conduct Root Cause Analysis of Suspicious Processes:** For each suspicious process (notepad++.exe, LibreViewMASMonitor.exe, and the other unidentified processes), perform a root cause analysis to determine how they were installed and whether they are benign. 5. **Regular Security Audits & Process Reviews:** Schedule regular security audits and process reviews to proactively identify and address potential vulnerabilities. This should include monitoring for new, unsigned processes and unusual network activity. **IMPORTANT NOTE:** This analysis is based solely on the provided scan data. Further investigation - including examining the files associated with the suspicious processes and reviewing network traffic - is required to fully understand the potential risks and implement more targeted mitigation strategies. A full malware scan with a reputable antivirus solution is strongly recommended to confirm the presence and nature of any malicious software.

Risk Assessment

Overall Risk Level: LOW - System appears secure