

A-Ryan Security Report

Generated on: 2025-09-26 19:01:15 ADT

Executive Summary

The security scan revealed a high level of risk due to multiple potentially suspicious processes and significant network activity. Several processes lack digital signatures, raising concerns about potential malware or unauthorized modifications. Immediate investigation and remediation are recommended to mitigate these identified vulnerabilities and maintain system security.

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': '2025-09-26T19:01:15.003299', 'total_processes': 230, 'suspicious_processes': 6,  
'high_resource_processes': 0, 'network_processes': 31, 'processes': [{'pid': 272, 'name': 'Registry',  
'exe_path': 'Registry', 'cmdline': '', 'cpu_percent': 0.0, 'memory_percent': 0.05969032316799018,  
'create_time': '2025-09-26T10:00:47.566587', 'username': None, 'status': 'running', 'num_threads': 4,  
'network_connections': 0, 'listening_ports': []}, {'pid': 296, 'name': 'chrome.exe', 'exe_path':  
'C:\\Program Files\\Google\\Chrome\\Application\\chrome.exe', 'cmdline': 'C:\\Program  
Files\\Google\\Chrome\\Application\\chrome.exe --type=renderer --no-pre-read-main-dll  
--video-capture-use-gpu-memory-buffer --lang=en-US --device-scale-factor=1  
--num-raster-threads=4 --enable-main-frame-before-activation --renderer-client-id=25  
--time-ticks-at-unix-epoch=-1758891647063880 --launch-time-ticks=29200423536  
--metrics-shmem-handle=7908,i,7796533523121335942,3072224860443501673,2097152  
--field-trial-handl... [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 230 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 `LibreViewMASMonitor.exe` (PID: 1984) and `Video.UI.exe` (PID: 9412) as these processes lack digital signatures and are exhibiting a high risk score. Utilize system monitoring tools and malware analysis techniques to determine the true nature of these processes and their legitimacy.

2. ****Full Antivirus Scan:**** Initiate a comprehensive full system scan using a reputable antivirus solution. This will detect and remove any malware or suspicious files associated with the identified processes or other areas of concern.

3. ****Review Network Connections:**** Conduct a detailed analysis of all network connections initiated by the scanned processes. Look for unusual or unauthorized communication patterns, which could indicate data exfiltration or command and control activity. Utilize network monitoring tools to identify and block suspicious traffic.

4. ****Digital Signature Verification:**** Verify the digital signatures of all critical system processes. Ensure all software installed on the system has a valid digital certificate from a trusted vendor. Investigate why some processes are missing these signatures.

5. ****Implement Enhanced System Monitoring:**** Deploy proactive system monitoring tools to track process behavior, network activity, and resource usage in real-time. Set alerts for deviations from baseline behavior, enabling rapid response to potential security incidents.

6. ****Regular Security Audits & Patch Management:**** Implement a regular schedule for security audits, vulnerability scanning, and patching. Ensure all software is up-to-date with the latest security patches.

Risk Assessment

Overall Risk Level: MEDIUM - Review and address issues