

ESL Pro Security Report

Generated on: 2025-09-14 18:20:20 ADT

Executive Summary

This security analysis reveals a HIGH risk posture due to the presence of suspicious processes and a non-digitally signed executable. Specifically, the anomalous execution of explorer.exe alongside a non-digitally signed process, LibreViewMASMonitor.exe, indicates a potential compromise or unauthorized activity. Immediate investigation and remediation are crucial to mitigate this risk.

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': '1,3-4,6-7,9,13,17,19-26,30,32-33,37,42-43,49,53,70,79-85,88-90,99-100,106,109-11,113,119,125,135,139,143-144,146,161,163,179,199,211-212,222,254-256,259,264,280,301,306,311,340,366,389,406-407,416-417,425,427,443-445,458,464-465,481,497,500,501,502,503,504,505,506,507,508,509,510,511,512,513,514,515,516,517,518,519,520,521,522,523,524,525,526,527,528,529,530,531,532,533,534,535,536,537,538,539,540,541,542,543,544,545,546,547,548,549,550,551,552,553,554,555,556,557,558,559,550-559,560-569,570-579,580-589,590-599,600-609,610-619,620-629,630-639,640-649,650-659,660-669,670-679,680-689,690-699,700-709,710-719,720-729,730-739,740-749,750-759,760-769,770-779,780-789,790-799,800-809,810-819,820-829,830-839,840-849,850-859,860-869,870-879,880-889,890-899,900-909,910-919,920-929,930-939,940-949,950-959,960-969,970-979,980-989,990-999,1000-1009,1010-1019,1020-1029,1030-1039,1040-1049,1050-1059,1060-1069,1070-1079,1080-1089,1090-1099,1100-1109,1110-1119,1120-1129,1130-1139,1140-1149,1150-1159,1160-1169,1170-1179,1180-1189,1190-1199,1200-1209,1210-1219,1220-1229,1230-1239,1240-1249,1250-1259,1260-1269,1270-1279,1280-1289,1290-1299,1300-1309,1310-1319,1320-1329,1330-1339,1340-1349,1350-1359,1360-1369,1370-1379,1380-1389,1390-1399,1400-1409,1410-1419,1420-1429,1430-1439,1440-1449,1450-1459,1460-1469,1470-1479,1480-1489,1490-1499,1500-1509,1510-1519,1520-1529,1530-1539,1540-1549,1550-1559,1560-1569,1570-1579,1580-1589,1590-1599,1600-1609,1610-1619,1620-1629,1630-1639,1640-1649,1650-1659,1660-1669,1670-1679,1680-1689,1690-1699,1700-1709,1710-1719,1720-1729,1730-1739,1740-1749,1750-1759,1760-1769,1770-1779,1780-1789,1790-1799,1800-1809,1810-1819,1820-1829,1830-1839,1840-1849,1850-1859,1860-1869,1870-1879,1880-1889,1890-1899,1900-1909,1910-1919,1920-1929,1930-1939,1940-1949,1950-1959,1960-1969,1970-1979,1980-1989,1990-1999,2000-2009,2010-2019,2020-2029,2030-2039,2040-2049,2050-2059,2060-2069,2070-2079,2080-2089,2090-2099,2100-2109,2110-2119,2120-2129,2130-2139,2140-2149,2150-2159,2160-2169,2170-2179,2180-2189,2190-2199,2200-2209,2210-2219,2220-2229,2230-2239,2240-2249,2250-2259,2260-2269,2270-2279,2280-2289,2290-2299,2300-2309,2310-2319,2320-2329,2330-2339,2340-2349,2350-2359,2360-2369,2370-2379,2380-2389,2390-2399,2400-2409,2410-2419,2420-2429,2430-2439,2440-2449,2450-2459,2460-2469,2470-2479,2480-2489,2490-2499,2500-2509,2510-2519,2520-2529,2530-2539,2540-2549,2550-2559,2560-2569,2570-2579,2580-2589,2590-2599,2600-2609,2610-2619,2620-2629,2630-2639,2640-2649,2650-2659,2660-2669,2670-2679,2680-2689,2690-2699,2700-2709,2710-2719,2720-2729,2730-2739,2740-2749,2750-2759,2760-2769,2770-2779,2780-2789,2790-2799,2800-2809,2810-2819,2820-2829,2830-2839,2840-2849,2850-2859,2860-2869,2870-2879,2880-2889,2890-2899,2900-2909,2910-2919,2920-2929,2930-2939,2940-2949,2950-2959,2960-2969,2970-2979,2980-2989,2990-2999,20000-20099,20100-20199,20200-20299,20300-20399,20400-20499,20500-20599,20600-20699,20700-20799,20800-20899,20900-20999,21000-21099,21100-21199,21200-21299,21300-21399,21400-21499,21500-21599,21600-21699,21700-21799,21800-21899,21900-21999,22000-22099,22100-22199,22200-22299,22300-22399,22400-22499,22500-22599,22600-22699,22700-22799,22800-22899,22900-22999,23000-23099,23100-23199,23200-23299,23300-23399,23400-23499,23500-23599,23600-23699,23700-23799,23800-23899,23900-23999,24000-24099,24100-24199,24200-24299,24300-24399,24400-24499,24500-24599,24600-24699,24700-24799,24800-24899,24900-24999,25000-25099,25100-25199,25200-25299,25300-25399,25400-25499,25500-25599,25600-25699,25700-25799,25800-25899,25900-25999,26000-26099,26100-26199,26200-26299,26300-26399,26400-26499,26500-26599,26600-26699,26700-26799,26800-26899,26900-26999,27000-27099,27100-27199,27200-27299,27300-27399,27400-27499,27500-27599,27600-27699,27700-27799,27800-27899,27900-27999,28000-28099,28100-28199,28200-28299,28300-28399,28400-28499,28500-28599,28600-28699,28700-28799,28800-28899,28900-28999,29000-29099,29100-29199,29200-29299,29300-29399,29400-29499,29500-29599,29600-29699,29700-29799,29800-29899,29900-29999,200000-200999,201000-201999,202000-202999,203000-203999,204000-204999,205000-205999,206000-206999,207000-207999,208000-208999,209000-209999,210000-210999,211000-211999,212000-212999,213000-213999,214000-214999,215000-215999,216000-216999,217000-217999,218000-218999,219000-219999,220000-220999,221000-221999,222000-222999,223000-223999,224000-224999,225000-225999,226000-226999,227000-227999,228000-228999,229000-229999,230000-230999,231000-231999,232000-232999,233000-233999,234000-234999,235000-235999,236000-236999,237000-237999,238000-238999,239000-239999,240000-240999,241000-241999,242000-242999,243000-243999,244000-244999,245000-245999,246000-246999,247000-247999,248000-248999,249000-249999,250000-250999,251000-251999,252000-252999,253000-253999,254000-254999,255000-255999,256000-256999,257000-257999,258000-258999,259000-259999,260000-260999,261000-261999,262000-262999,263000-263999,264000-264999,265000-265999,266000-266999,267000-267999,268000-268999,269000-269999,270000-270999,271000-271999,272000-272999,273000-273999,274000-274999,275000-275999,276000-276999,277000-277999,278000-278999,279000-279999,280000-280999,281000-281999,282000-282999,283000-283999,284000-284999,285000-285999,286000-286999,287000-287999,288000-288999,289000-289999,290000-290999,291000-291999,292000-292999,293000-293999,294000-294999,295000-295999,296000-296999,297000-297999,298000-298999,299000-299999,2000000-2009999,2010000-2019999,2020000-2029999,2030000-2039999,2040000-2049999,2050000-2059999,2060000-2069999,2070000-2079999,2080000-2089999,2090000-2099999,2100000-2109999,2110000-2119999,2120000-2129999,2130000-2139999,2140000-2149999,2150000-2159999,2160000-2169999,2170000-2179999,2180000-2189999,2190000-2199999,2200000-2209999,2210000-2219999,2220000-2229999,2230000-2239999,2240000-2249999,2250000-2259999,2260000-2269999,2270000-2279999,2280000-2289999,2290000-2299999,2300000-2309999,2310000-2319999,2320000-2329999,2330000-2339999,2340000-2349999,2350000-2359999,2360000-2369999,2370000-2379999,2380000-2389999,2390000-2399999,2400000-2409999,2410000-2419999,2420000-2429999,2430000-2439999,2440000-2449999,2450000-2459999,2460000-2469999,2470000-2479999,2480000-2489999,2490000-2499999,2500000-2509999,2510000-2519999,2520000-2529999,2530000-2539999,2540000-2549999,2550000-2559999,2560000-2569999,2570000-2579999,2580000-2589999,2590000-2599999,2600000-2609999,2610000-2619999,2620000-2629999,2630000-2639999,2640000-2649999,2650000-2659999,2660000-2669999,2670000-2679999,2680000-2689999,2690000-2699999,2700000-2709999,2710000-2719999,2720000-2729999,2730000-2739999,2740000-2749999,2750000-2759999,2760000-2769999,2770000-2779999,2780000-2789999,2790000-2799999,2800000-2809999,2810000-2819999,2820000-2829999,2830000-2839999,2840000-2849999,2850000-2859999,2860000-2869999,2870000-2879999,2880000-2889999,2890000-2899999,2900000-2909999,2910000-2919999,2920000-2929999,2930000-2939999,2940000-2949999,2950000-2959999,2960000-2969999,2970000-2979999,2980000-2989999,2990000-2999999,20000000-20099999,20100000-20199999,20200000-20299999,20300000-20399999,20400000-20499999,20500000-20599999,20600000-20699999,20700000-20799999,20800000-20899999,20900000-20999999,21000000-21099999,21100000-21199999,21200000-21299999,21300000-21399999,21400000-21499999,21500000-21599999,21600000-21699999,21700000-21799999,21800000-21899999,21900000-21999999,22000000-22099999,22100000-22199999,22200000-22299999,22300000-22399999,22400000-22499999,22500000-22599999,22600000-22699999,22700000-22799999,22800000-22899999,22900000-22999999,23000000-23099999,23100000-23199999,23200000-23299999,23300000-23399999,23400000-23499999,23500000-23599999,23600000-23699999,23700000-23799999,23800000-23899999,23900000-23999999,24000000-24099999,24100000-24199999,24200000-24299999,24300000-24399999,24400000-24499999,24500000-24599999,24600000-24699999,24700000-24799999,24800000-24899999,24900000-24999999,25000000-25099999,25100000-25199999,25200000-25299999,25300000-25399999,25400000-25499999,25500000-25599999,25600000-25699999,25700000-25799999,25800000-25899999,25900000-25999999,26000000-26099999,26100000-26199999,26200000-26299999,26300000-26399999,26400000-26499999,26500000-26599999,26600000-26699999,26700000-26799999,26800000-26899999,26900000-26999999,27000000-27099999,27100000-27199999,27200000-27299999,27300000-27399999,27400000-27499999,27500000-27599999,27600000-27699999,27700000-27799999,27800000-27899999,27900000-27999999,28000000-28099999,28100000-28199999,28200000-28299999,28300000-28399999,28400000-28499999,28500000-28599999,28600000-28699999,28700000-28799999,28800000-28899999,28900000-28999999,29000000-29099999,29100000-29199999,29200000-29299999,29300000-29399999,29400000-29499999,29500000-29599999,29600000-29699999,29700000-29799999,29800000-29899999,29900000-29999999,200000000-200999999,201000000-201999999,202000000-202999999,203000000-203999999,204000000-204999999,205000000-205999999,206000000-206999999,207000000-207999999,208000000-208999999,209000000-209999999,210000000-210999999,211000000-211999999,212000000-212999999,213000000-213999999,214000000-214999999,215000000-215999999,216000000-216999999,217000000-217999999,218000000-218999999,219000000-219999999,220000000-220999999,221000000-221999999,222000000-222999999,223000000-223999999,224000000-224999999,225000000-225999999,226000000-226999999,227000000-227999999,228000000-228999999,229000000-229999999,230000000-230999999,231000000-231999999,232000000-232999999,233000000-233999999,234000000-234999999,235000000-235999999,236000000-236999999,237000000-237999999,238000000-238999999,239000000-239999999,240000000-240999999,241000000-241999999,242000000-242999999,243000000-243999999,244000000-244999999,245000000-245999999,246000000-246999999,247000000-247999999,248000000-248999999,249000000-249999999,250000000-250999999,251000000-251999999,252000000-252999999,253000000-253999999,254000000-254999999,255000000-255999999,256000000-256999999,257000000-257999999,258000000-258999999,259000000-259999999,260000000-260999999,261000000-261999999,262000000-262999999,263000000-263999999,264000000-264999999,265000000-265999999,266000000-266999999,267000000-267999999,268000000-268999999,269000000-269999999,270000000-270999999,271000000-271999999,272000000-272999999,273000000-273999999,274000000-274999999,275000000-275999999,276000000-276999999,277000000-277999999,278000000-278999999,279000000-279999999,280000000-280999999,281000000-281999999,282000000-282999999,283000000-283999999,284000000-28499

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': '2025-09-14T18:20:20.203031', 'total_processes': 247, 'suspicious_processes': 6,  
'high_resource_processes': 1, 'network_processes': 35, 'processes': [{  
    'pid': 272, 'name': 'Registry',  
    'exe_path': 'Registry', 'cmdline': "", 'cpu_percent': 0.0, 'memory_percent': 0.07039259294143559,  
    'create_time': '2025-09-14T11:10:53.581732', 'username': None, 'status': 'running', 'num_threads': 4,  
    'network_connections': 0, 'listening_ports': []}, {  
    'pid': 368, 'name': 'ApplicationFrameHost.exe',  
    'exe_path': 'C:\Windows\System32\ApplicationFrameHost.exe', 'cmdline':  
        'C:\Windows\system32\ApplicationFrameHost.exe -Embedding', 'cpu_percent': 0.0,  
    'memory_percent': 0.07215801417022506, 'create_time': '2025-09-14T11:18:17.099874',  
    'username': 'DESKTOP-DUQ7M23\leaw0', 'status': 'running', 'num_threads': 33,  
    'network_connections': 0, 'listening_ports': [], 'file_size': 96504, 'file_modified':  
        '2025-04-25T18:10:17.261243', 'file_created': '2025-04-25T18:10:17.250240', 'file_hash_partial':  
        '43... [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 21 network connections

Process Security Analysis

Scanned 247 processes, found 6 suspicious processes. Process security risk level: HIGH

Key Process Findings:

Found 6 potentially suspicious processes

Susp
c:\wir

AI Security Recommendations

Detailed Analysis & Recommendations

1. ****Immediate Investigation of Explorer.exe (PID: 9260):**** Conduct a thorough analysis of the explorer.exe process, including its parent processes, network connections, and file modifications. Verify its legitimacy and determine the cause of its unusual execution location.

2. ****Scan for Malware Related to LibreViewMASMonitor.exe (PID: 10144):**** Due to the non-digital signed nature of this process, immediately execute a full system scan with a reputable antivirus program. This step is essential to rule out malware infection.

3. ****Verify Digital Signatures of All System Processes:**** Implement a policy requiring all system processes to be digitally signed by a trusted publisher. This will prevent unauthorized modifications and help detect malicious activity.

4. ****Enhanced Process Monitoring:**** Implement real-time monitoring of system processes, paying particular attention to resource usage and network connections. Configure alerts for unusual or excessive activity.

5. ****Strengthen Security Hygiene:**** Ensure all software is up-to-date with the latest security patches and updates. Regularly review and strengthen firewall rules and network security configurations.

Risk Assessment

Overall Risk Level: LOW - System appears secure