AI-Assisted Investigation Report

Analyst

MalwareLab User

Analysis Time

2026-07-16 19:38:03 (EDT - America/New_York) | 2026-07-16 23:38:03 UTC

Model

gpt-4.1-mini

Version

beta-v2.0

Report Metrics

Input Size: 64 bytes
IOCs Found: 2
ATT&CK Techniques: 0

Severity

High

Confidence

85% - Moderate Confidence

Confidence Factors

• 68 malicious detections on VirusTotal
• File identified as Win32 EXE with suspicious tags including exploit and CVE references
• Presence of digital signature from Microsoft Windows Operating System (signature verification unknown) increases scrutiny due to possible masquerade
• Negative reputation score (-1806) indicating poor trust

Reducing Factors

• Digital signature present from Microsoft Windows Operating System publisher
• Signature verification status unknown

Threat Type

Malware

Executive Summary

The file with SHA256 hash 24d004a104d4d54034dbcffc2a4b19a11f39008a575aa614ea04703480b1022c is a Win32 executable with a digital signature from Microsoft Windows Operating System (verification unknown). It has a high number of malicious detections (68) on VirusTotal and is tagged with exploit-related behaviors and CVE references, indicating likely malicious activity despite the signature.

Evidence Supporting Assessment

• VirusTotal reports 68 malicious detections and 0 harmless detections for the file
• File is a Win32 executable named lhdfrgui.exe
• Tags include exploit, cve-2017-0147, cve-2017-0144, and malware indicating exploit capabilities
• Digital signature is present but verification status is unknown, suggesting possible masquerade or signature tampering
• Negative reputation score (-1806) supports suspicion of maliciousness

Ambiguity Notes

• Signature verification status is unknown, limiting confidence in the trustworthiness of the digital signature
• MalwareBazaar did not find this hash, so no additional threat intelligence is available from that source
• No behavioral or telemetry data provided to confirm execution or impact

Alternative Hypotheses

• The file is a legitimate Microsoft Windows system file falsely flagged by some antivirus engines
• The file is a malware sample masquerading as a signed Microsoft Windows executable
• The file is a security research or penetration testing sample using a Microsoft signature for evasion

Alternative Explanations

None

Indicators of Compromise

Hashes
- 24d004a104d4d54034dbcffc2a4b19a11f39008a575aa614ea04703480b1022c

Processes
- lhdfrgui.exe

MITRE ATT&CK Mapping

None

Recommended Actions

• Investigate any occurrences of lhdfrgui.exe on endpoints and servers
• Verify the digital signature validity and origin of the file using trusted tools
• Perform behavioral analysis or sandbox execution to confirm malicious activity
• Search for exploitation attempts related to CVE-2017-0147 and CVE-2017-0144 in network and endpoint logs
• Quarantine and block execution of the file pending further analysis

Analyst Notes

None

AI-Assisted Analysis Disclaimer

This report was generated using AI-assisted analysis and is intended to support security investigations. Findings, conclusions, and recommendations should be reviewed and validated by a qualified analyst before operational, legal, or business decisions are made.

