Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

CVE-2025-11001 Turns a Simple Unzip into a System-Level Ambush

Date of Publication	Admiralty Code	TA Number
November 21, 2025	A1	TA2025356

Summary

First Seen: May 2025
Affected Product: 7-Zip Windows
Impact: CVE-2025-11001 is a 7-Zip directory traversal flaw that misprocesses symbolic links in ZIP files, allowing attackers to redirect extraction to unintended system paths and execute code on Windows systems with elevated privileges. Introduced in version 21.02 and fixed in version 25.00, it remains a high-risk vulnerability due to public proof-of-concept exploit availability.

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2025-11001	7-Zip Remote Code Execution Vulnerability	7-Zip	✗	✗	✓
CVE-2025-11002	7-Zip Remote Code Execution Vulnerability	7-Zip	✗	✗	✓

Vulnerability Details

#1 A recently disclosed 7-Zip flaw, tracked as CVE-2025-11001, is a directory traversal defect in the way 7-Zip processes symbolic links embedded in ZIP archives. Improper handling of these links allows a crafted archive to redirect extraction to unintended file system locations and execute code under the privileges of the affected service or user.

#2 A malicious ZIP can appear routine but contain symbolic links designed to mimic standard filesystem shortcuts. Instead of confining extraction to the target directory, the flaw allows these links to redirect 7-Zip to sensitive areas of the system, enabling file overwrites or unauthorized code execution.

#3 Attackers achieve this by embedding symbolic links that use Windows-style absolute paths, which 7-Zip incorrectly interprets as relative paths. During extraction, the application creates these links to arbitrary directories. Subsequent archive contents pass through the links and are written outside the intended extraction path, allowing system file modification or the placement of hostile payloads.

#4 The issue was introduced in 7-Zip version 21.02. CVE-2025-11001 and the related CVE-2025-11002 were both corrected in version 25.00, released in July 2025. CVE-2025-11001 affects only Windows systems and becomes exploitable when executed with elevated privileges or when Developer Mode is enabled. With confirmed publicly available proof-of-concept material, the vulnerability represents a significant operational risk.

Vulnerabilities

CVE ID	AFFECTED PRODUCT	AFFECTED CPE	CWE ID
CVE-2025-11001	7-Zip before version 25.00	cpe:2.3:a:7-zip:7-zip:*:*:*:*:*:*:*:*	CWE-22
CVE-2025-11002			

Recommendations

Software Hardening: Ensure all systems run 7Zip version 25.00, the first release that fully addresses CVE-2025-11001 and related flaws. Remove every older or duplicate installation to eliminate residual attack paths. Prevent use of unauthorized archive utilities by enforcing controlled software baselines across endpoints.

System Integrity Assurance: Conduct regular audits of system directories that are likely targets for overwrite attempts. Track unauthorized file modifications, new binaries, or abnormal write patterns. Integrate endpoint rules capable of detecting or blocking symlink-based traversal events and unauthorized payload placement.

Monitor Extraction Behavior: Check ZIP files for symbolic links before extraction. Detect and alert on any attempt to write files outside the target directory. Log all extraction activity on systems that handle sensitive data.

Potential MITRE ATT&CK TTPs

TA0002 Execution	**TA0003** Persistence	**TA0005** Defense Evasion	**TA0007** Discovery
T1059 Command and Scripting Interpreter	**T1204.002** Malicious File	**T1204** User Execution	**T1055** Process Injection
T1574 Hijack Execution Flow	**T1574.001** DLL	**T1036** Masquerading	**T1036.008** Masquerade File Type
T1083 File and Directory Discovery			

Patch Link

https://www.7-zip.org/download.html

References

https://digital.nhs.uk/cyber-alerts/2025/cc-4719

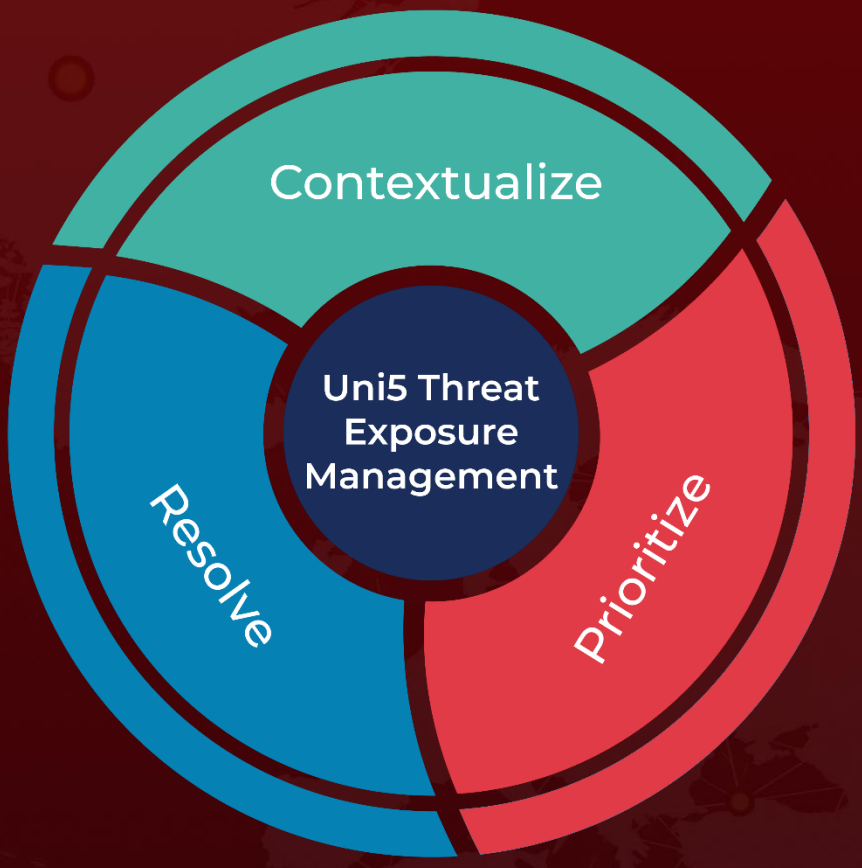
https://www.zerodayinitiative.com/advisories/ZDI-25-949/

https://github.com/pacbypass/CVE-2025-11001

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

November 21, 2025 . 09:00 AM

More at www.hivepro.com