مجلس الأمن السيبراني

CYBER SECURITY COUNCIL

United Arab Emirates

High-Severity Vulnerabilities in 7-Zip

Tracking #:432317807

Date:13-10-2025

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed high-severity vulnerabilities in the open-source compression utility 7-Zip, which could allow attackers to execute arbitrary code when a user opens or extracts a specially crafted ZIP file.

TECHNICAL DETAILS:

High-Severity vulnerabilities in the popular open-source compression utility 7-Zip, identified as CVE-2025-11001 and CVE-2025-11002. These flaws reside in the handling of symbolic links within ZIP archives and could be exploited by attackers to execute arbitrary code on affected systems.

Vulnerability Details

- CVE-2025-11001, CVE-2025-11002
- CVSS Score 7.0 Severity: High
- Impact: Remote Code Execution
- Attack Vector: User-assisted (malicious ZIP file)
- Both vulnerabilities result from improper handling of symbolic links inside ZIP archives. A specially crafted ZIP file can cause the extraction process to traverse outside the intended directory, potentially overwriting sensitive or executable files. When these files are later executed, attackers can achieve arbitrary code execution, possibly with elevated privileges — especially if 7-Zip operates in a service or privileged account context.
- Attackers may leverage these vulnerabilities to:
  - Overwrite configuration or startup files for persistence.
  - Drop malicious executables into trusted directories.
  - Execute code through overwritten files or services.
  - Distribute malicious ZIP files via phishing campaigns disguised as legitimate attachments (e.g., invoices, resumes, project files).
- Affected Product: 7-Zip prior to version 25.00
- Fixed Version: 7-Zip 25.00 or later

RECOMMENDATIONS:

- Update immediately to 7-Zip version 25.00 or later.
- Do not extract archives from untrusted sources.
- For automated/sandboxed extraction workflows, consider isolating such operations and monitoring for suspicious file writes outside intended directories.
- Audit access to trusted directories and file paths on systems processing untrusted ZIP files.
- Monitor for spawning of new files or scripts by 7-Zip processes

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://www.zerodayinitiative.com/advisories/ZDI-25-950/
- https://www.zerodayinitiative.com/advisories/ZDI-25-949/