مجلس الأمن السيبراني

CYBER SECURITY COUNCIL

United Arab Emirates

Arbitrary File Write Vulnerability in 7-Zip

Tracking #:432317588

Date:11-08-2025

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLGIENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a security vulnerability in 7-Zip that could potentially be exploited to execute malicious code on affected systems.

TECHNICAL DETAILS:

A security vulnerability has been identified in 7-Zip versions older than 25.01, where the software improperly handles symbolic links during archive extraction. Attackers can craft malicious archives that exploit this behavior to write files arbitrarily outside the intended extraction directory. This can lead to arbitrary code execution if the attacker overwrites sensitive configuration or executable files.

Vulnerability Details:

- **CVE-2025-55188**
- **Severity**: Low
- **CVSS v3 Score**: 3.6
- When extracting archives, 7-Zip follows symbolic links inside the archive. A malicious archive can exploit this to overwrite files outside the extraction directory. Attackers can overwrite sensitive files like SSH keys, .bashrc, or security configurations, which may allow them to execute code or maintain persistent access**.**
- Successful exploitation allows attackers to:
  - Overwrite critical files (e.g., SSH keys, .bashrc, startup scripts).
  - Establish persistent backdoors or execute arbitrary commands.
  - Bypass security controls by manipulating configuration files.

Affected Versions:

- 7-Zip versions prior to 25.01

Fixed Versions:

- 7-Zip 25.01 or later

RECOMMENDATIONS:

- **Update immediately** to 25.01 or later from the official 7-Zip website.
- Avoid extracting archives from untrusted sources.
- **Use sandboxed or isolated environments** when handling unknown files.

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://nvd.nist.gov/vuln/detail/CVE-2025-55188
- https://seclists.org/oss-sec/2025/q3/82