10 years CERT-EU

Security Advisory 2024-118

Critical Vulnerability in 7-Zip

2024-11-25 — v1.0

TLP:CLEAR

History:

- *25/11/2024 — v1.0 – Initial publication*

Summary

A severe security vulnerability has been discovered in 7-Zip, the popular file compression utility, allowing remote attackers to execute malicious code through specially crafted archives. The vulnerability tracked as **CVE-2024-11477** has received a high CVSS score of 7.8 [1].

Technical Details

This vulnerability allows remote attackers to execute arbitrary code on affected installations of 7-Zip. Interaction with this library is required to exploit this vulnerability but attack vectors may vary depending on the implementation [2].

The specific flaw exists within the implementation of `Zstandard` decompression. The issue results from the lack of proper validation of user-supplied data, which can result in an integer underflow before writing to memory. An attacker can leverage this vulnerability to execute code in the context of the current process [2].

Affected Products

The vulnerability was fixed in 7-Zip 24.07 [2].

Recommendations

CERT-EU recommends updating the software to the latest version.

References

[1] https://cybersecuritynews.com/7-zip-vulnerability-arbitrary-code/

[2] https://www.zerodayinitiative.com/advisories/ZDI-24-1532/