CERT-EU

Security Advisory 2024-095

Critical vulnerabilities in Adobe Products

2024-09-12 — v1.0

TLP:CLEAR

History:

- *12/09/2024 — v1.0 – Initial publication*

Summary

On September 10, 2024, Adobe released a security bulletin addressing two critical vulnerabilities affecting its Acrobat products. When exploited, these vulnerabilities could allow an attacker to execute arbitrary code [1].

A publicly available proof-of-concept exploit exists for one of the vulnerabilities [2].

Technical Details

The vulnerability **CVE-2024-41869**, with a CVSS score of 7.8, is a use after free flaw that could lead to remote code execution when opening a specially crafted PDF document. A proof-of-concept exploit exists for this vulnerability.

The vulnerability **CVE-2024-45112**, with a CVSS score of 8.6, is a type confusion vulnerability that could lead to remote code execution.

Affected Products

The following products are affected:

- Acrobat DC and Acrobat Reader DC for Windows versions 24.003.20054 and earlier.
- Acrobat DC and Acrobat Reader DC for MacOS versions 24.002.21005 and earlier.
- Acrobat 2024 for Windows and MacOS versions 24.001.30159 and earlier.
- Acrobat 2020 and Acrobat Reader 2020 for Windows and MacOS versions 20.005.30655 and earlier.

Recommendations

CERT-EU strongly recommends updating affected products to a fixed version [2].

References

[1] https://helpx.adobe.com/security/products/acrobat/apsb24-70.html

[2] https://www.bleepingcomputer.com/news/security/adobe-fixes-acrobat-reader-zero-day-with-public-poc-exploit/