10 years CERT-EU

Security Advisory 2024-022

Vulnerabilities in Adobe products

February 29, 2024 — v1.0

TLP:CLEAR

History:

- *29/02/2024 — v1.0 – Initial publication*

Summary

On February 13, 2024, Adobe released two security advisories addressing multiple high severity vulnerabilities [1, 2] in various Adobe products. If exploited, the vulnerabilities would allow an attacker to cause remote arbitrary code execution, remote denial of service, remote code injection or disclosure of sensitive information.

Technical Details

Among all the fixed vulnerabilities, the critical ones, with CVSS scores ranging from 7.8 to 9.1 out of 10, are due to:

- Improper neutralisation of special elements used in an OS command (CVE-2024-20720 - CVSS 9.1);
- Cross-site scripting (CVE-2024-20719 - CVSS 9.1);
- Out-of-bounds write (CVE-2024-20726, CVE-2024-20727, CVE-2024-20728 - CVSS 7.8);
- Use after free (CVE-2024-20729, CVE-2024-20765, CVE-2024-20731 - CVSS 7.8 and CVSS 8.8);
- Integer overflow or wraparound (CVE-2024-20730 - CVSS 7.8).

If exploited, these critical vulnerabilities could lead to arbitrary code execution.

Affected Products

- Adobe Commerce version 2.4.6-x prior to 2.4.6-p4
- Adobe Commerce version 2.4.5-x prior to 2.4.5-p6
- Adobe Commerce version 2.4.4-x prior to 2.4.4-p7
- Adobe Commerce version 2.4.3-x prior to 2.4.3-ext-6
- Adobe Commerce version 2.4.2-x prior to 2.4.2-ext-6
- Adobe Commerce version 2.4.1-x prior to 2.4.1-ext-6
- Adobe Commerce version 2.4.0-x prior to 2.4.0-ext-6
- Adobe Commerce version 2.3.7-x prior to 2.3.7-p4-ext-6
- Magento Open Source versions 2.4.6-x prior to 2.4.6-p4
- Magento Open Source versions 2.4.5-x prior to 2.4.5-p6
- Magento Open Source versions 2.4.4-x prior to 2.4.4-p7

- Acrobat DC versions prior to 23.008.20533 on Windows and macOS
- Acrobat Reader DC versions prior to 23.008.20533 on Windows and macOS
- Acrobat 2020 versions prior to 20.005.30574 on Windows and macOS
- Acrobat Reader 2020 versions prior to 20.005.30574 on Windows and macOS

Recommendations

CERT-EU strongly recommends updating software installations to the latest versions by following the instructions given by the vendor [1,2].

References

[1] https://helpx.adobe.com/security/products/magento/apsb24-03.html

[2] https://helpx.adobe.com/security/products/acrobat/apsb24-07.html

[3] https://blog.talosintelligence.com/vulnerability-roundup-feb-27-2024/