Severity

High

Analysis Summary

CVE-2022-24105 CVSS:7.8

Adobe Photoshop could allow a remote attacker to execute arbitrary code on the system, caused by an out-of-bounds write error. By persuading a victim to open a specially-crafted document, a remote attacker could exploit this vulnerability to execute arbitrary code on the system with the privileges of the victim or cause the application to crash.

CVE-2022-28279 CVSS:7.8

Adobe Photoshop could allow a remote attacker to execute arbitrary code on the system, caused by a use-after-free error. By persuading a victim to open a specially-crafted document, a remote attacker could exploit this vulnerability to execute arbitrary code on the system with the privileges of the victim or cause the application to crash.

CVE-2022-28278 CVSS:7.8

Adobe Photoshop could allow a remote attacker to execute arbitrary code on the system, caused by an out-of-bounds write error. By persuading a victim to open a specially-crafted document, a remote attacker could exploit this vulnerability to execute arbitrary code on the system with the privileges of the victim or cause the application to crash.

CVE-2022-28277 CVSS:7.8

Adobe Photoshop could allow a remote attacker to execute arbitrary code on the system, caused by an out-of-bounds write error. By persuading a victim to open a specially-crafted document, a remote attacker could exploit this vulnerability to execute arbitrary code on the system with the privileges of the victim or cause the application to crash.

CVE-2022-28276 CVSS:7.8

Adobe Photoshop could allow a remote attacker to execute arbitrary code on the system, caused by an out-of-bounds write error. By persuading a victim to open a specially-crafted document, a remote attacker could exploit this vulnerability to execute arbitrary code on the system with the privileges of the victim or cause the application to crash.

CVE-2022-28275 CVSS:7.8

Adobe Photoshop could allow a remote attacker to execute arbitrary code on the system, caused by an out-of-bounds write error. By persuading a victim to open a specially-crafted document, a remote attacker could exploit this vulnerability to execute arbitrary code on the system with the privileges of the victim or cause the application to crash.

CVE-2022-28274 CVSS:7.8

Adobe Photoshop could allow a remote attacker to execute arbitrary code on the system, caused by an out-of-bounds write error. By persuading a victim to open a specially-crafted document, a remote attacker could exploit this vulnerability to execute arbitrary code on the system with the privileges of the victim or cause the application to crash.

CVE-2022-28273 CVSS:7.8

Adobe Photoshop could allow a remote attacker to execute arbitrary code on the system, caused by an out-of-bounds write error. By persuading a victim to open a specially-crafted document, a remote attacker could exploit this vulnerability to execute arbitrary code on the system with the privileges of the victim or cause the application to crash.

CVE-2022-28272 CVSS:7.8

Adobe Photoshop could allow a remote attacker to execute arbitrary code on the system, caused by a use-after-free error. By persuading a victim to open a specially-crafted document, a remote attacker could exploit this vulnerability to execute arbitrary code on the system with the privileges of the victim or cause the application to crash.

CVE-2022-28271 CVSS:7.8

Adobe Photoshop could allow a remote attacker to execute arbitrary code on the system, caused by a use-after-free error. By persuading a victim to open a specially-crafted document, a remote attacker could exploit this vulnerability to execute arbitrary code on the system with the privileges of the victim or cause the application to crash.

CVE-2022-28270 CVSS:7.8

Adobe Photoshop could allow a remote attacker to execute arbitrary code on the system, caused by an out-of-bounds write error. By persuading a victim to open a specially-crafted document, a remote attacker could exploit this vulnerability to execute arbitrary code on the system with the privileges of the victim or cause the application to crash.

CVE-2022-24093 CVSS:9.1

Adobe Commerce and Magento Open Source allow a remote attacker to execute arbitrary code on the system, caused by improper input validation. By sending a specially-crafted request, an attacker could exploit this vulnerability to execute arbitrary code on the system.

CVE-2022-27784 CVSS:7.8

Adobe After Effects is vulnerable to a stack-based buffer overflow, caused by improper bounds checking when processing video files. By persuading a victim to open a specially-crafted file, a remote attacker could overflow a buffer and execute arbitrary code in the context of the current process.

CVE-2022-27783 CVSS:7.8

Adobe After Effects is vulnerable to a stack-based buffer overflow, caused by improper bounds checking when processing video files. By persuading a victim to open a specially-crafted file, a remote attacker could overflow a buffer and execute arbitrary code in the context of the current process.

CVE-2022-23205 CVSS:7.8

Adobe Photoshop could allow a remote attacker to execute arbitrary code on the system, caused by an out-of-bounds write error. By persuading a victim to open a specially-crafted document, a remote attacker could exploit this vulnerability to execute arbitrary code on the system with the privileges of the victim or cause the application to crash.

CVE-2022-24098 CVSS:7.8

Adobe Photoshop could allow a remote attacker to execute arbitrary code on the system, caused by improper validation of input. By persuading a victim to open a specially-crafted document, a remote attacker could exploit this vulnerability to execute arbitrary code on the system with the privileges of the victim or cause the application to crash.

CVE-2022-28279 CVSS:7.8

Adobe Photoshop could allow a remote attacker to execute arbitrary code on the system, caused by a use-after-free error. By persuading a victim to open a specially-crafted document, a remote attacker could exploit this vulnerability to execute arbitrary code on the system with the privileges of the victim or cause the application to crash.

Impact

- Code Execution
- Buffer Overflow

Indicator Of Compromise

CVE

- CVE-2022-24105
- CVE-2022-28279
- CVE-2022-28278
- CVE-2022-28277
- CVE-2022-28276
- CVE-2022-28275
- CVE-2022-28274
- CVE-2022-28273
- CVE-2022-28272
- CVE-2022-28271
- CVE-2022-28270
- CVE-2022-24093
- CVE-2022-27784
- CVE-2022-27783
- CVE-2022-23205
- CVE-2022-24098
- CVE-2022-28279

Affected Vendors

- Adobe

Affected Products

- Adobe Photoshop 2021 22.5.6
- Adobe Photoshop 2022 23.2.2
- Adobe Commerce 2.4.3-p1
- Adobe Commerce 2.3.7-p2
- Adobe Magento Open Source 2.4.3-p1
- Adobe Magento Open Source 2.3.7-p2
- Adobe After Effects 22.2.1
- Adobe After Effects 18.4.5

Remediation

Refer to Adobe Security Advisory for patch, upgrade, or suggested workaround information.

[Adobe Photoshop](#)

[Adobe Commerce and Magento Open Source](#)

[Adobe After Effects](#)