



CVE-2023-21578

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

| | |
|------------------------|---|
| CVE | CVE-2023-21578 |
| State | PUBLIC |
| Assigner | psirt@adobe.com |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2023-02-17 22:15:00 UTC |
| Updated | 2023-02-24 23:50:00 UTC |
| Description | Photoshop version 23.5.3 (and earlier), 24.1 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to |

Risk And Classification

Problem Types: CWE-125

NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|------------------|---------------------------|---------------------------|---------|--------|---------|----------|
| Application | Adobe | Photoshop | All | All | All | All |
| Operating System | Apple | Macos | - | All | All | All |
| Operating System | Microsoft | Windows | - | All | All | All |

References

| Reference | Source | Link | Tags |
|--------------------------|---------|---|---------------------|
| Adobe Security Bulletin | MISC | helpx.adobe.com | |
| CVE Program record | CVE.ORG | www.cve.org | canonical |
| NVD vulnerability detail | NVD | nvd.nist.gov | canonical, analysis |

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[377979](#) Adobe Photoshop Arbitrary Code Execution Vulnerability (APSB23-11)

completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report