

**Overall Rating: High**

**This is a technical bulletin intended for technical audiences.**

## Summary

The Vulnerability and Risk Management (VRM) Team has been made aware Adobe published security advisories to address vulnerabilities in the following products:

- Acrobat 2024 – version 24.001.30123 and prior
- Acrobat 2020 – version 20.005.30636 and prior (Windows), version 20.005.30635 and prior (MacOS)
- Acrobat DC – version 24.002.20991 and prior (Windows), version 24.002.20964 and prior (MacOS)
- Acrobat Reader 2020 – version 20.005.30636 and prior (Windows), version 20.005.30635 and prior (MacOS)
- Acrobat Reader DC – version 24.002.20991 and prior (Windows), version 24.002.20964 and prior (MacOS)
- Adobe Bridge – version 13.0.8 and prior, version 14.1.1 and prior
- Adobe Commerce – multiple versions
- Adobe Dimension – version 3.4.11 and prior
- Adobe InCopy – version 19.4 and prior, version 18.5.2 and prior
- Adobe InDesign – version ID19.4 and prior, version ID18.5.2 and prior
- Adobe Substance 3D Designer – version 13.1.2 and prior
- Adobe Substance 3D Sampler – version 4.5 and prior
- Adobe Substance 3D Stager – version 3.0.2 and prior
- Illustrator 2024 – version 28.5 and prior
- Illustrator 2023 – version 27.9.4 and prior
- Magento Open Source – multiple versions
- Photoshop 2023 – version 24.7.3 and prior
- Photoshop 2024 – version 25.9.1 and prior

## Technical Details

Review the latest information about available product updates as well as guidance on security issues reported about our products.

Title	Originally posted	Last updated
<a href="#">APSB24-45 : Security update available for Adobe Illustrator</a>	08/13/2024	08/13/2024
<a href="#">APSB24-47 : Security update available for Adobe Dimension</a>	08/13/2024	08/13/2024
<a href="#">APSB24-49 : Security update available for Adobe Photoshop</a>	08/13/2024	08/13/2024
<a href="#">APSB24-56 : Security update available for Adobe InDesign</a>	08/13/2024	08/13/2024

<a href="#">APSB24-57 : Security update available for Adobe Acrobat Reader</a>	08/13/2024	08/13/2024
<a href="#">APSB24-59 : Security update available for Adobe Bridge</a>	08/13/2024	08/13/2024
<a href="#">APSB24-60 : Security update available for Adobe Substance 3D Stager</a>	08/13/2024	08/13/2024
<a href="#">APSB24-61 : Security update available for Adobe Commerce</a>	08/13/2024	08/13/2024
<a href="#">APSB24-64 : Security update available for Adobe InCopy</a>	08/13/2024	08/13/2024
<a href="#">APSB24-65 : Security update available for Adobe Substance 3D Sampler</a>	08/13/2024	08/13/2024
<a href="#">APSB24-67 : Security update available for Adobe Substance 3D Designer</a>	08/13/2024	08/13/2024

This vulnerability is rated as a **HIGH** risk. A software update exists to address this risk.

### Action Required

- Locate the device or application and investigate.
- Notify business owner(s).
- Perform mitigating actions, as required.

Please notify [VRM](#) with any questions or concerns you may have at [vulnerabilityandriskmanagement@gov.bc.ca](mailto:vulnerabilityandriskmanagement@gov.bc.ca)

### References

- CVE-2024-34133 CVE-2024-34118 CVE-2024-34134 CVE-2024-34135 CVE-2024-34136 CVE-2024-34137 CVE-2024-34124 CVE-2024-41865 CVE-2024-20789 CVE-2024-34125 CVE-2024-34126 CVE-2024-20790 CVE-2024-20753 CVE-2024-39389 CVE-2024-39390 CVE-2024-39391 CVE-2024-41852 CVE-2024-41853 CVE-2024-39393 CVE-2024-39394 CVE-2024-41850 CVE-2024-41851 CVE-2024-39395 CVE-2024-34127 CVE-2024-41854 CVE-2024-41866 CVE-2024-39383 CVE-2024-39422 CVE-2024-39423 CVE-2024-39424 CVE-2024-39425 CVE-2024-39426 CVE-2024-41830 CVE-2024-41831 CVE-2024-41832 CVE-2024-41833 CVE-2024-41834 CVE-2024-41835 CVE-2024-39386 CVE-2024-41840 CVE-2024-39387 CVE-2024-39388 CVE-2024-41858 CVE-2024-41860 CVE-2024-41861 CVE-2024-41862 CVE-2024-41863 CVE-2024-41864
- [Adobe Security Advisories](#)