Adobe Security Bulletin

Last updated on Apr 28, 2026

Security updates available for Substance 3D Designer | APSB26-19

Bulletin ID	Date Published	Priority
APSB26-19	February 10, 2026	3

Summary

Adobe has released an update for Adobe Substance 3D Designer that addresses critical and important vulnerabilities. Successful exploitation could lead to arbitrary code execution, application denial-of-service, and memory exposure in the context of the current user.

Adobe is not aware of any exploits in the wild for any of the issues addressed in these updates.

Affected Versions

Product	Version	Platform
Adobe Substance 3D Designer	15.1.1 and earlier versions	All

Solution

Adobe categorizes these updates with the following priority ratings and recommends users update their installation to the newest version via the Creative Cloud desktop app's update mechanism. For more information, please reference this help page.

Product	Version	Platform	Priority	Availability
Adobe Substance 3D Designer	15.1.2	All	3	Download Center

For managed environments, IT administrators can use the Admin Console to deploy Creative Cloud applications to end users. Refer to this help page for more information.

Vulnerability Details

Vulnerability Category	Vulnerability Impact	Severity	CVSS base score	CVSS vector
Out-of-bounds Write (CWE-787)	Arbitrary code execution	Critical	7.8	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
Out-of-bounds Write (CWE-787)	Arbitrary code execution	Critical	7.8	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
NULL Pointer Dereference (CWE-476)	Application denial-of-service	Important	5.5	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H
Out-of-bounds Read (CWE-125)	Memory exposure	Important	5.5	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N

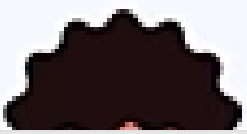
NULL Pointer Dereference (CWE-476)	Application denial-of-service	Important	5.5	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N
Out-of-bounds Read (CWE-125)	Memory exposure	Important	5.5	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N
Out-of-bounds Read (CWE-125)	Memory exposure	Important	5.5	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N

Acknowledgments:

Adobe would like to thank the following researchers for reporting the relevant issues and for working with Adobe to help protect our customers:

- voidexploit -- CVE-2026-21334, CVE-2026-21335, CVE-2026-21336, CVE-2026-21337, CVE-2026-21338, CVE-2026-21339, CVE-2026-21340

NOTE: Adobe has a public bug bounty program with HackerOne. If you are interested in working with



Was this page helpful? Yes, thanks | Not really

Ask the Community

Post questions and get answers from experts.

Ask now

Contact Us

Expert support for your issues.

Start now

^ Back to top