Adobe

Sign in

Adobe Security Bulletin

Security Updates Available for Adobe Acrobat and Reader | APSB20-48

Bulletin ID	Date Published	Priority
APSB20-48	August 11, 2020	2

ON THIS PAGE

Last Published: **August 28, 2020**

Summary

Adobe has released security updates for Adobe Acrobat and Reader for Windows and macOS. These updates address critical and important vulnerabilities. Successful exploitation could lead to arbitrary code execution in the context of the current user.

Affected Versions

Product	Track	Affected Versions
Acrobat DC	Continuous	2020.009.20074 and earlier versions
Acrobat Reader DC	Continuous	2020.009.20074 and earlier versions

Acrobat 2020	Classic 2020	2020.001.30002	
Acrobat Reader 2020	Classic 2020	2020.001.30002	
Acrobat 2017	Classic 2017	2017.011.30171 and earlier versions	
Acrobat Reader 2017	Classic 2017	2017.011.30171 and earlier versions	
Acrobat 2015	Classic 2015	2015.006.30523 and earlier versions	
Acrobat Reader 2015	Classic 2015	2015.006.30523 and earlier versions	

Solution

Adobe recommends users update their software installations to the latest versions by following the instructions below.

The latest product versions are available to end users via one of the following methods:

- Users can update their product installations manually by choosing Help > Check for Updates.
- The products will update automatically, without requiring user intervention, when updates are detected.

- The full Acrobat Reader installer can be downloaded from the Acrobat Reader Download Center.

For IT administrators (managed environments):

- Download the enterprise installers from ftp://ftp.adobe.com/pub/adobe/, or refer to the specific release note version for links to installers.
- Install updates via your preferred methodology, such as AIP-GPO, bootstrapper, SCUP/SCCM (Windows), or on macOS, Apple Remote Desktop and SSH.

Adobe categorizes these updates with the following priority ratings and recommends users update their installation to the newest version:

Product	Track	**Updated Versions**	**Platform**	**Priorit Rating**
Acrobat DC	Continuous	2020.012.20041	Windows and macOS	2
Acrobat Reader DC	Continuous	2020.012.20041	Windows and macOS	2
Acrobat 2020	Classic 2020	2020.001.30005	Windows and macOS	2
Acrobat Reader 2020	Classic 2020	2020.001.30005	Windows and macOS	2

Acrobat 2017	Classic 2017	2017.011.30175	Windows and macOS	2
Acrobat Reader 2017	Classic 2017	2017.011.30175	Windows and macOS	2
Acrobat 2015	Classic 2015	2015.006.30527	Windows and macOS	2
Acrobat Reader 2015	Classic 2015	2015.006.30527	Windows and macOS	2

Vulnerability Details

Vulnerability Category	Vulnerability Impact	Severity	CVE Number
Disclosure of Sensitive Data	Memory Leak	Important	CVE-2020-9697
Security bypass	Privilege Escalation	Important	CVE-2020-9714
Out-of-bounds write	Arbitrary Code Execution	Critical	CVE-2020-9693 CVE-2020-9694
Security bypass	Security feature	Critical	CVE-2020-9696

	bypass		CVE-2020-9712
Stack exhaustion	Application denial-of-service	Important	CVE-2020-9702 CVE-2020-9703
Out-of-bounds read	Information disclosure	Important	CVE-2020-9723 CVE-2020-9705 CVE-2020-9706 CVE-2020-9707 CVE-2020-9710 CVE-2020-9716 CVE-2020-9717 CVE-2020-9718 CVE-2020-9719 CVE-2020-9720 CVE-2020-9721
Buffer error	Arbitrary Code Execution	Critical	CVE-2020-9698

			CVE-2020-9699 CVE-2020-9700 CVE-2020-9701 CVE-2020-9704
Use-after-free	Arbitrary Code Execution	Critical	CVE-2020-9715 CVE-2020-9722
Memory corruption	Arbitrary Code Execution	Critical	CVE-2020-9713 CVE-2020-9695
Memory corruption	Information disclosure	Important	CVE-2020-9711

Acknowledgements

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

- Anonymous working with Trend Micro Zero Day Initiative (CVE-2020-9693, CVE-2020-9694)
- Steven Seeley of Qihoo 360 Vulcan Team (CVE-2020-9723)
- Abdul-Aziz Hariri of Trend Micro Zero Day Initiative (CVE-2020-9697, CVE-2020-9706, CVE-2020-9707, CVE-2020-9710, CVE-2020-9712)

- Csaba Fitzl (@theevilbit) from Offensive Security working with iDefense Labs (CVE-2020-9714)
- Kyle Martin from North Carolina State University, Sung Ta Dinh from Arizona State University, Haehyun Cho from Arizona State University, Ruoyu "Fish" Wang from Arizona State University, Alexandros Kapravelos from North Carolina State University and Yan Shoshitaishvili from Arizona State University (CVE-2020-9722)
- Ken Hsu of Palo Alto Networks. (CVE-2020-9695)
- Zhangqing, Zhiyuan Wang and willJ from cdsrc of Qihoo 360 (CVE-2020-9716, CVE-2020-9717, CVE-2020-9718, CVE-2020-9719, CVE-2020-9720, CVE-2020-9721)
- Mark Vincent Yason (@MarkYason) working with Trend Micro Zero Day Initiative (CVE-2020-9715)
- Xinyu Wan, Yiwei Zhang and Wei You from Renmin University of China (CVE-2020-9705, CVE-2020-9711, CVE-2020-9713)
- Xu Peng from TCA/SKLCS Institute of Software Chinese Academy of Sciences and Wang Yanhao from QiAnXin Technology Research Institute (CVE-2020-9698, CVE-2020-9699, CVE-2020-9700, CVE-2020-9701, CVE-2020-9702, CVE-2020-9703, CVE-2020-9704)
- Yuebin Sun(@yuebinsun) of Tencent Security Xuanwu Lab (CVE-2020-9696)

Revisions

August 25, 2020: Updated acknowledgement for CVE-2020-9722.

August 28, 2020: Included details about CVE-2020-9713, CVE-2020-9695, CVE-2020-9711.

^ Back to top

Ask the Community

Post questions and get answers from experts.

Ask now

Contact Us

Expert support for your issues.

Start now

Was this page helpful? Yes No