

CERT-EU Security Advisory 2018-015

Critical Vulnerabilities in Adobe Acrobat, Reader and Photoshop CC

May 15, 2018 — v1.0

History:

- 15/05/2018 — v1.0: Initial publication

Summary

Adobe has released Adobe Security Bulletins APSB18-09 and APSB18-17 [3] providing security updates [1, 2] for Adobe Acrobat, Reader and Adobe Photoshop CC for Windows and MacOS. These updates address **critical and important vulnerabilities**, which successful exploitation could lead to **arbitrary code execution** in the context of the current user.

Technical Details

Critical vulnerabilities addressed:

- Double free – Arbitrary Code Execution, CVE-2018-4990
- Heap overflow – Arbitrary Code execution, CVE-2018-4947, CVE-2018-4948, CVE-2018-4966, CVE-2018-4968, CVE-2018-4978, CVE-2018-4982, CVE-2018-4984
- Use-after-free – Arbitrary Code Execution, CVE-2018-4946, CVE-2018-4952, CVE-2018-4954, CVE-2018-4958, CVE-2018-4959, CVE-2018-4961, CVE-2018-4971, CVE-2018-4974, CVE-2018-4977, CVE-2018-4980, CVE-2018-4983, CVE-2018-4988, CVE-2018-4989
- Out-of-bounds write – Arbitrary Code Execution, CVE-2018-4950
- Type confusion – Arbitrary Code Execution, CVE-2018-4953
- Untrusted pointer dereference – Arbitrary Code Execution, CVE-2018-4987
- Out-of-bounds write – Remote Code Execution, CVE-2018-4946 (Adobe Photoshop CC)

Important vulnerabilities addressed:

- Security Bypass – Information Disclosure, CVE-2018-4979
- Out-of-bounds read, – Information Disclosure, CVE-2018-4949, CVE-2018-4951, CVE-2018-4955, CVE-2018-4956, CVE-2018-4957, CVE-2018-4960, CVE-2018-4962, CVE-2018-4963, CVE-2018-4964, CVE-2018-4967, CVE-2018-4969, CVE-2018-4970, CVE-2018-4972, CVE-2018-4973, CVE-2018-4975, CVE-2018-4976, CVE-2018-4981, CVE-2018-4986, CVE-2018-4985
- Memory Corruption – Information Disclosure, CVE-2018-4965
- NTLM SSO hash theft – Information Disclosure, CVE-2018-4993
- HTTP POST new line injection via XFA submission – Security Bypass, CVE-2018-4994

Products Affected

- Acrobat DC – 2018.011.20038 and earlier versions (Windows and macOS)
- Acrobat Reader DC – 2018.011.20038 and earlier versions (Windows and macOS)
- Acrobat 2017 – 2017.011.30079 and earlier versions (Windows and macOS)
- Acrobat Reader 2017 DC – 2017.011.30079 and earlier versions (Windows and macOS)
- Acrobat DC (Classic 2015) – 2015.006.30417 and earlier versions (Windows and macOS)
- Acrobat Reader DC (Classic 2015) – 2015.006.30417 and earlier versions (Windows and macOS)
- Photoshop CC 2018 – 19.1.3 and earlier (Windows and macOS)
- Photoshop CC 2017 – 18.1.3 and earlier (macOS)
- Photoshop CC 2017 – 18.1.2 and earlier (Windows)

Recommendations

Adobe recommends users to update their software installations to the latest versions by following the instructions in [1, 2].

References

[1] <https://helpx.adobe.com/security/products/acrobat/apsb18-09.html>

[2] <https://helpx.adobe.com/security/products/photoshop/apsb18-17.html>

[3] <https://helpx.adobe.com/security.html>