**Alert – Adobe Vulnerabilities**

**Description:**
Adobe has released security updates for Adobe Acrobat and Reader for Windows and MacOS. These updates address critical and important vulnerabilities.

**Impact of the vulnerabilities:**
Successful exploitation could lead to arbitrary code execution in the context of the current user.

**Vulnerable or affected versions:**

| Product | Track | Affected Versions | Platform |
|---|---|---|---|
| Acrobat DC | Continuous | 2019.008.20081 and earlier versions | Windows |
| Acrobat DC | Continuous | 2019.008.20080 and earlier versions | macOS |
| Acrobat Reader DC | Continuous | 2019.008.20081 and earlier versions | Windows |
| Acrobat Reader DC | Continuous | 2019.008.20080 and earlier versions | macOS |
| | | | |
| Acrobat 2017 | Classic 2017 | 2017.011.30106 and earlier version | Windows |
| Acrobat 2017 | Classic 2017 | 2017.011.30105 and earlier version | macOS |
| Acrobat Reader 2017 | Classic 2017 | 2017.011.30106 and earlier version | Windows |
| Acrobat Reader 2017 | Classic 2017 | 2017.011.30105 and earlier version | macOS |
| | | | |
| Acrobat DC | Classic 2015 | 2015.006.30457 and earlier versions | Windows |
| Acrobat DC | Classic 2015 | 2015.006.30456 and earlier versions | macOS |
| Acrobat Reader DC | Classic 2015 | 2015.006.30457 and earlier versions | Windows |
| Acrobat Reader DC | Classic 2015 | 2015.006.30456 and earlier versions | macOS |

**Solution:**

Rw-CSIRT is strongly recommending **users** to:

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.

**Affected users should**: contact RW-CSIRT: Call **4045** or write to **security@risa.rw** to help for analyzing the source of the incident and recommendation.

**Vulnerability Details:**
https://helpx.adobe.com/security/products/acrobat/apsb18-41.html#VulnerabilityDetails

**References:**
https://helpx.adobe.com/security/products/acrobat/apsb18-41.html

**National Computer Security and Incident Response Team (Rw-CSIRT) Mission**

Rw-CSIRT mission is to build cyber-security capabilities to increase the capacity of "early **Detection**, **Prevention**, **Response** to incidents and **Reduce** Vulnerability" and raise cyber security awareness in public.