GOVERNMENT OF THE REPUBLIC OF VANUATU

PRIME MINISTER'S OFFICE

CERTVU
DEPARTMENT OF COMMUNICATIONS & DIGITAL TRANSFORMATION

PM B 9108 Port Vila, Vanuatu

Tel: (678) 33380

GOUVERNEMENT DE LA REPUBLIQUE DU VANUATU

BUREAU DU PREMIER MINISTRE

CERTVU

DEPARTMENT DE COMMUNICATION ET DE TRANSFORMATION NUMERIQUE

SPP 9108 Port Vila, Vanuatu
Tel: (678) 33380

23 April 2026

Advisory 134: Adobe Acrobat Use-After-Free Vulnerability (CVE-2020-9715).

Release Date: 13th April 2026
Impact: HIGH / CRITICAL
TLP: CLEAR

The Department of Communications and Digital Transformation (DCDT) through CERT Vanuatu (CERTVU), provides the following advisory.

This alert is relevant to Organizations and System/Network administrators that utilize the above products. This alert is intended to be understood by technical users and systems administrators.

What is it?

CVE-2020-9715 is a critical remote code execution (RCE) vulnerability in Adobe Acrobat Reader DC and Adobe Acrobat.

The flaw is a use-after-free memory corruption vulnerability (CWE-416) that occurs when the application improperly handles objects in memory while processing specially crafted PDF files. When freed memory is accessed again, attackers can manipulate it to execute arbitrary code.

What are the systems affected?

The vulnerability impacts;

- Adobe Acrobat Reader DC (versions prior to August 2020 updates)
- Adobe Acrobat (various desktop versions)
- Platforms: Windows and MacOS

What does this mean?

Exploitation is typically file-based and requires user interaction.

Typical attack flow:

1. **Delivery of malicious PDF**
    - The attacker crafts a specially designed PDF file containing exploit code.
    - Delivered via phishing emails, malicious downloads, or compromised websites.
2. **User opens the PDF**
    - The victim opens the file using a vulnerable version of Acrobat/Reader.
3. **Triggering the use-after-free flaw**
    - The PDF triggers improper memory handling in the application.
4. **Memory corruption**
    - Freed memory is reused and manipulated by the attacker.
5. **Arbitrary code execution**
    - Malicious code executes with the privileges of the current user.

Successful exploitation of this vulnerability may allow attackers to:

- Execute arbitrary code on the victim's system
- Install malware (e.g., spyware, trojans)
- Steal sensitive data
- Gain persistent access to the system
- Use the compromised system as a foothold for further attacks

The impact depends on the privileges of the user opening the file—higher privileges increase severity.

Mitigation process

CERTVU recommends the following:

Apply Adobe Security Updates (Critical)

- Update to the latest versions of:
    - **Adobe Acrobat Reader DC**
    - **Adobe Acrobat**
- Install patches released in August 2020 (APSB20-48 advisory) or later.

Reference

1. https://www.cisa.gov/known-exploited-vulnerabilities-catalog
2. https://www.cve.org/CVERecord?id=CVE-2020-9715
3. https://cwe.mitre.org/data/definitions/416.html
4. https://helpx.adobe.com/security/products/acrobat/apsb20-48.html