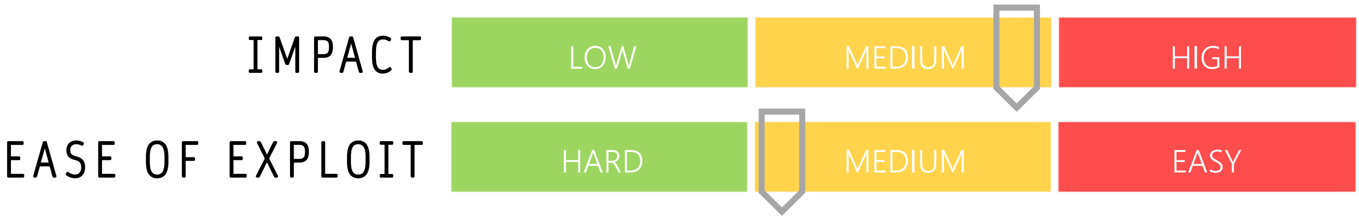
UNISPHERE SOLUTIONS

info@unisphere.co.nz
www.unisphere.co.nz

# CYBER GUIDANCE ISSUE 00105

## ADBOE EXPLOIT TARGETS WINDOWS USERS

DATE ISSUED: 15th February 2021



## OVERVIEW

A critical vulnerability in Adobe Reader that is susceptible to a heap-based buffer overflow attack is being actively exploited in an effort to target Microsoft Windows users. (CVE-2021-21017)

## BREAKDOWN

The "heap" is an area of a process's memory that stores dynamic variables and when it is "swamped" results in a buffer overflow causing the application to behave improperly which in this case can lead to the execution of arbitrary code on an affected system in the context of the current user.

Software version affected include:

- Acrobat Reader DC versions 2020.013.20074 and earlier for Windows and macOS
- Acrobat Reader 2020 versions 2020.001.30018 and earlier for Windows and macOS
- Acrobat Reader 2017 versions 2017.011.30188 and earlier for Windows and macOS

## REMEDIATION STEPS

- Apply security patches available as a part of the February update release to all Windows and macOS devices using Adobe Reader.

## REFERENCES & RESOURCES

| | |
|---|---|
| Threatpost: | https://threatpost.com/critical-adobe-windows-flaw/163789/ |
| ARS Technica | https://arstechnica.com/information-technology/2021/02/zerodays-under-active-exploit-are-keeping-windows-users-busy/ |