安全漏洞通告

Adobe Acrobat Reader 多个严重漏洞通告

360CERT
北京奇虎科技有限公司 | 2021-05-12

报告信息

报告名称	Adobe Acrobat Reader 多个严重漏洞通告		
报告类型	安全漏洞通告	**报告编号**	B6-2021-051202
报告版本	1	**报告日期**	2021-05-12
报告作者	360CERT	**联系方式**	cert@360.cn
提供方	北京奇虎科技有限公司		
接收方			

报告修订记录

报告版本	日期	修订	审核	描述
1	2021-05-12	360CERT	360CERT	撰写报告

目录

一、 漏洞档案 1
二、 漏洞简述 2
三、 漏洞评级 3
四、 漏洞详情 4
五、 影响版本 7
六、 漏洞列表 8
七、 安全建议 9
(一) 通用修补方案 9
八、 产品侧解决方案 11
(一) 360 安全卫士 11
(二) 360 安全卫士团队版 11
(三) 360 本地安全大脑 12
九、 参考链接 13
附录 A 报告风险等级说明 14
附录 B 影响面说明 16
附录 C 360 内部评分体系 17

一、 漏洞档案

漏洞类型	UAF 等
CVE 编号	CVE-2021-28550 等
相关厂商	adobe
相关组件	acrobat reader 2020 等
威胁等级	严重
影响面	广泛
360CERT 评分	9.8
修复方案	通用修补方案
漏洞发布时间	2021-05-12
报告生成时间	2021-05-12

二、 漏洞简述

2021 年 05 月 12 日，360CERT 监测发现 Adobe 发布了 Adobe Acrobat Reader 安全更新 的风险通告，其中涉及到 10 个严重漏洞，事件等级：严重，事件评分：9.8。

Adobe Acrobat Reader 是由 Adobe 公司所开发的电子文字处理软件集，可用于阅读、编辑、管理和共享 PDF 文档。 一般包含如下包： Adobe Acrobat Reader，包括专业版和标准版。用于对 PDF 文件进行编辑、共享和管理，需要购买，而 3D 版本，除了专业版的功能，另外也支持立体向量图片的转换。

对此，360CERT 建议广大用户及时将 Adobe Acrobat Reader 升级到最新版本。与此同时，请做好资产自查以及预防工作，以免遭受黑客攻击。

三、 漏洞评级

经过安全技术人员的分析，最终对该漏洞的评定结果如下

评定方式	等级
威胁等级	严重
影响面	广泛
360CERT 评分	9.8

四、 漏洞详情

CVE-2021-28550/28562/28553: Acrobat Reader UAF 漏洞

CVE: CVE-2021-28550、CVE-2021-28562、CVE-2021-28553

组件: acrobat reader dc,acrobat reader 2020,acrobat reader 2017

漏洞类型: UAF

影响:任意代码执行

简述: 利用此漏洞的攻击者，通过发送精心制造的 PDF 给受影响的 Acrobat 或 Reader 用户，可直接造成任意代码执行，获得终端控制权。此漏洞监测到存在在野利用，各厂商用户请及时更新

CVE-2021-21044/21038/21086: Acrobat Reader 内存越界写漏洞

CVE: CVE-2021-21044、CVE-2021-21038、CVE-2021-21086

组件: acrobat reader dc,acrobat reader 2017,acrobat reader 2020

漏洞类型: 内存越界写

影响: 任意代码执行

简述: 利用此漏洞的攻击者，通过提供精心构造的数据，可在当前进程的上下文中执行代码。

CVE-2021-28564: Acrobat Reader 内存越界写漏洞

CVE: CVE-2021-28564

组件: acrobat reader 2017,acrobat reader dc,acrobat reader 2020

漏洞类型：内存越界写

影响：任意代码执行

简述：利用此漏洞的攻击者，通过提供精心构造的数据，可在当前进程的上下文中执行代码。

CVE-2021-28565: Acrobat Reader 内存越界读漏洞

CVE: CVE-2021-28565

组件: acrobat reader 2020,acrobat reader 2017,acrobat reader dc

漏洞类型：内存越界读

影响：任意代码执行

简述：利用此漏洞的攻击者，通过提供精心构造的数据，可在当前进程的上下文中执行代码。

CVE-2021-28557: Acrobat Reader 内存越界读漏洞

CVE: CVE-2021-28557

组件: acrobat reader dc,acrobat reader 2020,acrobat reader 2017

漏洞类型：内存越界读

影响：内存泄漏

简述：利用此漏洞的攻击者，通过提供精心构造的数据，可造成内存泄漏。

CVE-2021-28560: Acrobat Reader 缓冲区溢出漏洞

CVE: CVE-2021-28560

组件: acrobat reader 2020,acrobat reader dc,acrobat reader 2017

漏洞类型: 缓冲区溢出

影响: 任意代码执行

简述: 利用此漏洞的攻击者，通过提供精心构造的数据，可造成任意代码执行

五、 影响版本

产品名称	影响版本
Adobe:Acrobat Reader DC	<=2021.001.20149
Adobe:Acrobat Reader 2020	<=2020.001.30020
Adobe:Acrobat Reader 2017	<=2017.011.30194

六、 漏洞列表

编号	描述	导致结果	威胁等级
CVE-2021-28550	use_after_free	任意代码执行	严重
CVE-2021-28562	use_after_free	任意代码执行	严重
CVE-2021-28553	use_after_free	任意代码执行	严重
CVE-2021-21044	内存越界读	任意代码执行	严重
CVE-2021-21038	内存越界读	任意代码执行	严重
CVE-2021-21086	内存越界读	任意代码执行	严重
CVE-2021-28564	内存越界读	任意代码执行	严重
CVE-2021-28565	内存越界读	任意代码执行	严重
CVE-2021-28557	内存越界读	内存泄漏	严重
CVE-2021-28560	缓冲区溢出	任意代码执行	严重

七、 安全建议

(一) 通用修补方案

最新的产品版本可通过以下方法提供给用户:

- 用户可以通过选择“帮助”>“检查更新”来手动更新其产品安装。

- 检测到更新后，产品将自动更新，而无需用户干预。

- 完整的 Acrobat Reader 安装程序可以从 Acrobat Reader 下载中心下载，下载链接: https://get.adobe.com/cn/reader/。

对于 IT 管理员（托管环境）:

- 请参阅特定的发行说明版本以获取安装程序的链接。

- 通过常用的方式进行更新，如 AIP-GPO、bootstrapper、SCUP/SCCM (Windows)、SSH、Apple Remote Desktop 等。

相关版本更新链接:

- Acrobat DC: https://www.adobe.com/devnet-docs/acrobatetk/tools/ReleaseNotesDC/index.html#continuous-track

- Acrobat Reader DC: https://www.adobe.com/devnet-docs/acrobatetk/tools/ReleaseNotesDC/index.html#continuous-track

- Acrobat 2020: https://www.adobe.com/devnet-docs/acrobatetk/tools/ReleaseNotesDC/index.html#classic-track

- Acrobat Reader 2020: https://www.adobe.com/devnet-docs/acrobatetk/tools/ReleaseNotesDC/index.html#classic-track

- Acrobat 2017: https://www.adobe.com/devnet-docs/acrobatetk/tools/ReleaseNotesDC/index.html#id3

- Acrobat Reader 2017: https://www.adobe.com/devnet-docs/acrobatetk/tools/ReleaseNotesDC/index.html#id3

八、 产品侧解决方案

(一) 360 安全卫士

针对本次安全更新，Windows 用户可通过 360 安全卫士实现对应补丁安装，其他平台的用户可以根据修复建议列表中的产品更新版本对存在漏洞的产品进行更新。如有其他问题可联系相关产品负责人或（360safe-ent#360.cn）。

(二) 360 安全卫士团队版

用户可以通过安装 360 安全卫士并进行全盘杀毒来维护计算机安全。360CERT 建议广大用户使用 360 安全卫士定期对设备进行安全检测，以做好资产自查以及防护工作。

(三) 360 本地安全大脑

360 本地安全大脑是将 360 云端安全大脑核心能力本地化部署的一套开放式全场景安全运营平台，实现安全态势、监控、分析、溯源、研判、响应、管理的智能化安全运营赋能。360 本地安全大脑已支持对相关漏洞利用的检测，请及时更新网络神经元（探针）规则和本地安全大脑关联分析规则，做好防护。

九、 参考链接

1. https://helpx.adobe.com/security/products/acrobat/apsb21-29.html

https://helpx.adobe.com/security/products/acrobat/apsb21-29.html

附录 A 报告风险等级说明

360CERT 评分是依托 CVSS3.1 的评价体系，由 360CERT 进行分数评定的危害评分

严重	
评定标准	1. 9.0 ≤ 360CERT 评分 ≤ 10 2. Top20 组件 3. PoC/Exp 公开可直接利用 4. 获得系统权限 5. 蠕虫性攻击
危害结果	1. 任意攻击者可直接发起攻击 2. 直接获得服务器控制权限 3. 直接影响业务服务运行 4. 核心敏感数据泄漏 5. 下载任意文件 6. 易造成资金风险
修复建议	建议在 3 个工作日内对涉及的产品/组件进行修复操作

高危	
评定标准	1. 7.0 ≤ 360CERT 评分 < 9 2. 通用组件 3. PoC 公开 4. 获得服务/数据库权限
危害结果	1. 系统/服务/资源垂直越权 2. 获得数据库权限 3. 可造成资金风险
修复建议	建议在 7 个工作日内对涉及的产品/组件进行修复操作

中危	
评定标准	1. 4.0 ≤ 360CERT 评分 < 7 2. 需要额外的操作步骤方可实现攻击 3. 对服务的运行产生影响但不影响功能 a) 占用存储空间 b) 降低执行效率 4. 获得平台用户级权限
危害结果	1. 需要额外的操作步骤实现危害行为 2. 获得平台平行越权 3. 任意文件上传 4. 难造成资金风险
修复建议	建议在 12 个工作日内对涉及的产品/组件进行修复操作

低危	
评定标准	1. 0 ≤ 360CERT 评分 < 4 2. 不对服务的运行产生影响
危害结果	暂无
修复建议	建议在 20 个工作日内对涉及的产品/组件进行修复操作

附录 B 影响面说明

影响面说明	
广泛	影响主体数 > 10w 底层依赖库
一般	5w < 影响主体数 < 10w 开源库
局限	影响主体数 < 5w 特制版本的

附录 C 360 内部评分体系

360 内部评分体系是 360CERT 安全研究人员经过一系列的数据分析和调查研究，并结合多年的漏洞研究经验最终得出的一套针对漏洞和安全事件的科学评分标准。此套评分体系能够用来评测漏洞和安全事件的严重程度，并帮助确定所需反应的紧急度和重要度。经验证，此评分体系适用于市面上几乎所有的漏洞和安全事件。

360 内部评分体系建立在"CVSS 漏洞评分体系"的基础上，其最终分数是取决于多个指标的公式，最终计算得出的近似的漏洞利用容易程度和漏洞利用的影响。分数范围是 0 到 10，其中最严重的是 10。该分数能较直观地反映漏洞的威胁等级，具体对应规则如下：

分数	威胁等级
9.0 – 10.0	严重
7.0 – 8.9	高危
4.0 – 6.9	中危
0 - 3.9	低危