安全漏洞通告

Autodesk 多个高危漏洞通告

360CERT
北京奇虎科技有限公司

报告信息

报告名称	Autodesk 多个高危漏洞通告		
报告类型	安全漏洞通告	报告编号	B6-2021-062401
报告版本	1	报告日期	2021-06-24
报告作者	360CERT	联系方式	g-cert-report@360.cn
提供方	北京鸿腾智能科技有限公司-360CERT		
接收方			

报告修订记录

报告版本	日期	修订	审核	描述
1	2021-06-24	360CERT	360CERT	撰写报告

目录

1 漏洞简述 4
2 风险等级 5
3 漏洞详情 6
CVE-2021-27033: Design Review 内存多重释放漏洞 6
CVE-2021-27034: Design Review 缓冲区溢出漏洞 6
CVE-2021-27035: Design Review 内存越界漏洞 6
CVE-2021-27036: Design Review 内存越界写漏洞 7
CVE-2021-27037: Design Review UAF 漏洞 7
CVE-2021-27038: Design Review 类型混淆漏洞 8
CVE-2021-27039: Design Review 内存越界漏洞 8
4 影响版本 9
5 修复建议 10
通用修补建议 10
6 时间线 11
7 参考链接 12
附录 13
A 产品侧解决方案 13
360 安全分析响应平台 13
360 安全卫士 13
360 本地安全大脑 14
360 终端安全管理系统 14

B 报告等级说明 16
严重 16
高危 16
中危 17
低危 18
C 影响面说明 20
D 360CERT 内部评分体系 21

1 漏洞简述

2021 年 06 月 24 日，360CERT 监测发现 06 月 14 日 Autodesk 发布了 DesignReview安全更新通告，本次安全更新中修复了 7 处漏洞，漏洞等级：高危，漏洞评分：8.9。

Autodesk 是在建筑、工程及制造业等行业的产品闻名软件公司，其拥有 AutoCAD，AutoCAD WS，Autodesk Alias，Autodesk Maya，Autodesk Design Review 等多款软件，在全世界范围内拥有大量的客户。攻击者可以通过利用这些漏洞构造一个恶意的网页或文件诱使用户点击，从而控制用户的主机。

Autodesk 系列产品通常用在企业内网的员工办公机上，攻击者通常会使用社会工程学的方式将身份伪装成求职者等其他身份向企业员工发送包含恶意代码的文件，当企业员工运行该文件时，攻击者便可在员工主机上直接执行任意代码，从而突破企业边界防御策略，直接入侵到企业办公网段。但是内存漏洞存在利用成本高、触发情况不稳定的情况，同时该漏洞需要用户参与点击，利用难度中。

对此，360CERT 建议广大用户及时将 AutodeskDesignReview 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。

2 风险等级

360CERT 对该漏洞的评定结果如下

评定方式	等级
威胁等级	高危
影响面	广泛
攻击者价值	非常高
利用难度	中
360CERT 评分	8.9

3 漏洞详情

3.1 CVE-2021-27033: Design Review 内存多重释放漏洞

CVE: CVE-2021-27033
组件: Design Review
漏洞类型: 内存多重释放
影响: 接管用户计算机
简述: Autodesk Design Review 对 PDF 的处理过程中存在多重释放漏洞。攻击者通过诱使用户打开特制的网页或 PDF 文件，可利用该漏洞控制用户计算机。

3.2 CVE-2021-27034: Design Review 缓冲区溢出漏洞

CVE: CVE-2021-27034
组件: Design Review
漏洞类型: 缓冲区溢出
影响: 接管用户计算机
简述: Autodesk Design Review 解析 PICT 或 TIFF 文件过程中存在基于堆的缓冲区溢出漏洞。攻击者通过诱使用户打开特制的 PICT 或 TIFF 文件，可利用该漏洞控制用户计算机。

3.3 CVE-2021-27035: Design Review 内存越界漏洞

CVE: CVE-2021-27035
组件: Design Review
漏洞类型: 内存越界
影响: 接管用户计算机

简述: Autodesk Design Review 解析 TIFF、PDF、PICT 或 DWF 文件时存在内容越界读取写入漏洞。攻击者通过诱使用户打开特制的 TIFF、PDF、PICT 或 DWF 文件，可利用该漏洞控制用户计算机。

3.4 CVE-2021-27036: Design Review 内存越界写漏洞

CVE: CVE-2021-27036
组件: Design Review
漏洞类型: 内存越界写
影响: 接管用户计算机
简述: Autodesk Design Review 解析 PDF、PICT 或 TIFF 文件时存在内容越界写入漏洞。攻击者通过诱使用户打开特制的 PDF、PICT 或 TIFF 文件，可利用该漏洞控制用户计算机。

3.5 CVE-2021-27037: Design Review UAF 漏洞

CVE: CVE-2021-27037
组件: Design Review
漏洞类型: UAF
影响: 接管用户计算机
简述: Autodesk Design Review 解析 PNG、PDF 或 DWF 文件时存在 (UAF) 内存释放后使用漏洞。攻击者通过诱使用户打开特制的 PNG、PDF 或 DWF 文件，可利用该漏洞控制用户计算机。

3.6 CVE-2021-27038: Design Review 类型混淆漏洞

CVE: CVE-2021-27038

组件: Design Review

漏洞类型: 类型混淆

影响: 接管用户计算机

简述: Autodesk Design Review 解析 PDF 文件时存在类型混淆漏洞。攻击者通过诱使用户打开特制的网页、PDF 文件，可利用该漏洞控制用户计算机。

3.7 CVE-2021-27039: Design Review 内存越界漏洞

CVE: CVE-2021-27039

组件: Design Review

漏洞类型: 内存越界

影响: 接管用户计算机

简述: Autodesk Design Review 解析 TIFF 文件时存在内容越界读写漏洞。攻击者通过诱使用户打开特制的 TIFF 文件，可利用该漏洞控制用户计算机。

4 影响版本

软件	影响版本	安全版本
Autodesk Design Review	2011	2018 Hotfix 3
Autodesk Design Review	2012	2018 Hotfix 3
Autodesk Design Review	2013	2018 Hotfix 3
Autodesk Design Review	2017	2018 Hotfix 3
Autodesk Design Review	2018	2018 Hotfix 3
Autodesk Design Review	2018_hotfix_1	2018 Hotfix 3
Autodesk Design Review	2018_hotfix_2	2018 Hotfix 3

5 修复建议

5.1 通用修补建议

Autodesk® Design Review 2013 或更早版本的客户需要按照 Autodesk 知识网络中的安装说明升级到 2018 或更高版本。使用不再有获得全面支持的版本（<2013）的客户应计划尽快升级到受支持的版本，以避免受到安全漏洞影响。

6 时间线

2021-06-14 Autodesk 发布通告

2021-06-24 360CERT 发布通告

7 参考链接

Vulnerabilities in the Autodesk® Design Review software

A 产品侧解决方案

若想了解更多产品信息或有相关业务需求，可移步至 http://360.net。

A.1 360 安全分析响应平台

360 安全大脑的安全分析响应平台通过网络流量检测、多传感器数据融合关联分析手段，对该类漏洞的利用进行实时检测和阻断，请用户联系相关产品区域负责人或(shaoyulong#360.cn) 获取对应产品。

A.2 360 安全卫士

Windows 用户可通过 360 安全卫士实现对应补丁安装、漏洞修复、恶意软件查杀，其他平台的用户可以根据修复建议列表中的安全建议进行安全维护。
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。

A.3 360 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。

A.4 360 终端安全管理系统

360 终端安全管理系统软件是在 360 安全大脑极智赋能下，以大数据、云计算等新技术为支撑，以可靠服务为保障，集防病毒与终端安全管控功能于一体的企业级安全

产品。

360 终端安全管理系统已支持对相关漏洞进行检测和修复，建议用户及时更新漏洞库并安装更新相关补丁。

360终端安全管理系统软件是在360安全大脑极智赋能下，以大数据、云计算等新技术为支撑，以可靠服务为保障，集防病毒与终端安全管控功能于一体的企业级安全产品。

360终端安全管理系统已支持对相关漏洞进行检测和修复，建议用户及时更新漏洞库并安装更新相关补丁。

B 报告等级说明

360CERT 评分是依托于 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. 实施攻击成本低，难度低 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

C 影响面说明

影响面说明	
广泛	1. 影响主体数 > 10w 2. 底层依赖库
一般	1. 5w < 影响主体数 < 10w 2. 次级开源库
局限	1. 影响主体数 < 5w 2. 特制版本的

D 360CERT 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