安全漏洞通告

CVE-2021-30116: Kaseya VSA 远程代码执行漏洞通告

360CERT
北京奇虎科技有限公司

报告信息

报告名称	CVE-2021-30116: Kaseya VSA 远程代码执行漏洞通告		
报告类型	安全漏洞通告	报告编号	B6-2021-070601
报告版本	1	报告日期	2021-07-06
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	2021-07-06	360CERT	360CERT	撰写报告

目录

1 漏洞简述

2021 年 07 月 06 日，360CERT 监测发现 Kaseya 发布了 VSA管理软件 的风险通告，漏洞等级：严重，漏洞评分：9.8。

Kaseya VSA 是一款企业用于集中 IT 管理的软件。分为管理端和用户端，管理端可以批量的控制用户端设备，例如在用户端设备上执行命令、执行脚本、开启/关闭电源等。

根据其官方通告以及监测到的 REvil 利用 VSA 漏洞的勒索事件，VSA 软件中存在多个严重漏洞。攻击者可以利用这些漏洞绕过身份验证直接控制 VSA 管理端，并可通过管理端进一步控制其下属设备。

对此，360CERT 建议广大用户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	严重
影响面	广泛
攻击者价值	极高
利用难度	低
360CERT 评分	9.8

3 漏洞详情

3.1 CVE-2021-30116: VSA SQL 注入漏洞

CVE: CVE-2021-30116

组件: VSA

漏洞类型: SQL 注入；代码执行

影响: 服务器接管

简述: VSA 管理程序 Endpoint 中存在多处 SQL 注入漏洞，该漏洞位于userFilterTableRpt.asp，通过相连接的 SQL Server 攻击者可以通过执行恶意查询语句，借此执行系统命令以及.net 代码。

3.2 CVE-2021-30116: VSA 身份验证绕过漏洞

CVE: CVE-2021-30116

组件: VSA

漏洞类型: 代码执行

影响: 绕过身份验证限制使用服务所提供功能；服务器接管

简述: VSA 管理程序的 Endpoint 中存在一处身份验证绕过漏洞，该漏洞位于 dl.asp 路由，并可以与该路由下的其他路径功能相组合使用。

3.3 CVE-2021-30116: VSA 文件上传漏洞

CVE: CVE-2021-30116

组件: VSA

漏洞类型: 文件上传

影响: 上传恶意文件至服务器；服务器接管

简述：VSA 管理程序的 Endpoint 中存在一处任意文件上传漏洞，该漏洞位于KUpload.dll，该上传漏洞的成因是正常的上传功能与身份验证漏洞的结合，导致攻击者可以借此攻陷系统。

4 影响版本

组件	影响版本	安全版本
Kaseya:VSA	*	暂无

5 修复建议

5.1 通用修补建议

暂无

5.2 临时修补建议

Kaseya 官方建议用户在发布更新修复程序之前按照以下步骤进行处置

- 断开本地 VSA 服务器的网络连接，并保持设备的离线
- 使用官方提供的检测脚本，针对 VSA 受控的下属设备进行检测

Kaseya 官方检测程序下载

6 时间线

2021-07-04 DIVD CSIRT 发布通告

2021-07-05 Kaseya 发布通告

2021-07-06 360CERT 发布通告

7 参考链接

KASEYA CASE UPDATE 2

Important Notice July 5th, 2021

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 城市级网络安全监测服务

360CERT 的安全分析人员利用 360 安全大脑的 QUAKE 资产测绘平台 (quake.360.cn)，通过资产测绘技术的方式，对该漏洞进行监测。可联系相关产品区域负责人或 (quake#360.cn) 获取对应产品。

A.2 360 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.3 360 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