安全漏洞通告

飞利浦 Vue PACS 医学诊断系统多个高危漏洞通告

360CERT
北京奇虎科技有限公司

报告信息

报告名称	飞利浦 Vue PACS 医学诊断系统多个高危漏洞通告		
报告类型	安全漏洞通告	报告编号	B6-2021-071201
报告版本	1	报告日期	2021-07-12
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	2021-07-12	360CERT	360CERT	撰写报告

目录

1 漏洞简述

2021 年 07 月 12 日，360CERT 监测发现 飞利浦 发布了 VuePACS诊疗平台 的多个安全漏洞通告，漏洞编号为 CVE-2021-33020等 ，漏洞等级：严重，漏洞评分：9.8。

飞利浦 Vue PACS 诊断平台属于公共医疗健康领域的基础设施，该平台中存在多个可远程攻击利用的高危漏洞，影响范围广泛，攻击者通过这些漏洞极易获得患者敏感信息以及影响医疗过程，极易造成严重危害。

对此，360CERT 建议广大用户及时将 飞利浦VuePACS诊疗平台 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	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-2021-33020: 安全配置漏洞

CVE: CVE-2021-33020

组件: Vue PACS,Vue MyVue,Vue Speech,Vue Motion

漏洞类型: 安全配置

影响: 敏感信息泄漏；信息伪造

简述: 飞利浦 Vue PACS 诊疗平台仍在使用过期的安全密钥，这导致攻击者可以利用以往被泄漏的密钥针对现有的系统发起攻击

3.2 CVE-2021-27501: 安全配置漏洞

CVE: CVE-2021-27501

组件: Vue Motion,Vue PACS,Vue MyVue,Vue Speech

漏洞类型: 安全配置

影响: 代码执行；服务器接管

简述: 飞利浦 Vue PACS 诊疗平台的代码未遵循代码安全规则，导致攻击者可以利用这些代码逻辑错误对平台实施攻击

3.3 CVE-2021-33018: 安全配置漏洞

CVE: CVE-2021-33018

组件: Vue Speech,Vue Motion,Vue MyVue,Vue PACS

漏洞类型: 安全配置

影响: 敏感信息泄漏；信息伪造

简述: 飞利浦 Vue PACS 诊疗平台仍在使用存在安全隐患的加密算法，这导致攻击者

可以利用针对加密算法的漏洞对平台发起攻击

3.4 CVE-2021-27497: 安全防护缺陷漏洞

CVE: CVE-2021-27497
组件: Vue Motion,Vue PACS,Vue Speech,Vue MyVue
漏洞类型: 安全防护缺陷
影响: 系统中缺乏基础安全防护能力；服务器接管
简述: 飞利浦 Vue PACS 诊疗平台在安全性上存在重大隐患，其未使用充分的安全措施来保障平台的正确运行。

3.5 CVE-2021-27493: 数据未校验漏洞

CVE: CVE-2021-27493
组件: Vue PACS,Vue Motion,Vue MyVue,Vue Speech
漏洞类型: 数据未校验
影响: 执行非预期功能
简述: 飞利浦 Vue PACS 诊疗平台在接受数据时，未针对数据进行严格的字段校验，导致不受信任、危险的数据在平台内部流转。攻击者通过构造特制的请求包可在平台上执行非预期的功能。

3.6 CVE-2021-33024: 身份信息明文传输漏洞

CVE: CVE-2021-33024
组件: Vue Speech,Vue MyVue,Vue Motion,Vue PACS
漏洞类型: 身份信息未加密

影响: 身份信息泄漏

简述: 飞利浦 Vue PACS 诊疗平台在传输以及存储身份凭证时，使用了不安全的方式(未加密)。导致攻击者通过嗅探、拦截网络流量可直接获得平台相关身份凭据，并借此登录平台实施进一步攻击

3.7 CVE-2021-33022: 明文传输漏洞

CVE: CVE-2021-33022

组件: Vue Motion,Vue PACS,Vue Speech,Vue MyVue

漏洞类型: 明文传输

影响: 敏感信息泄漏

简述: 飞利浦 Vue PACS 诊疗平台在通信过程中以明文形式传输敏感或安全关键数据，未经授权的攻击者可以在互联网中嗅探到该数据中的详细信息。

4 影响版本

组件	影响版本	安全版本
Philips:Vue PACS	12.2.x.x	暂无
Philips:Vue MyVue	12.2.x.x	暂无
Philips:Vue Speech	12.2.x.x	暂无
Philips:Vue Motion	12.2.1.5	暂无

5 修复建议

5.1 通用修补建议

飞利浦 Vue PACS 诊疗平台可通过联系飞利浦地区服务支持中心获得相关技术支持。

飞利浦地区服务支持中心联系地址

5.2 临时修补建议

- 及时开启飞利浦 Vue 平台的自动更新功能
- 在安装更新后，断开飞利浦 Vue 平台和互联网的连接，保证只能通过内部网络进行登录访问
- 使用防火墙隔离飞利浦 Vue 平台，使其与个人终端互通受限

6 时间线

2021-06-29 飞利浦发布基础通告

2021-07-06 飞利浦发布正式通告

2021-07-12 360CERT 发布通告

7 参考链接

ICS Medical Advisory (ICSMA-21-187-01)

飞利浦安全通告

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 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.4 360 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.5 360 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