安全漏洞通告

CVE-2021-3044: Cortex XSOAR 未认证 REST API 使用漏洞通告

360CERT
北京奇虎科技有限公司

报告信息

报告名称	CVE-2021-3044: Cortex XSOAR 未认证 REST API 使用漏洞通告		
报告类型	安全漏洞通告	报告编号	B6-2021-062302
报告版本	1	报告日期	2021-06-23
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	2021-06-23	360CERT	360CERT	撰写报告

目录

1 漏洞简述

2021 年 06 月 23 日，360CERT 监测发现PaloAlto发布了CortexXSOAR未认证RESTAPI使用的风险通告，漏洞编号为 CVE-2021-3044 ，漏洞等级：严重，漏洞评分：9.8。Cortex XSOAR 是 Palo Alto 公司的 SOAR（安全编排自动化与相应）产品，其主要作用是跨源提取报警信息并执行自动化的工作流以加快事件响应速度，在世界范围内有大量客户。未认证的攻击者可以通过该漏洞访问 Cortex XSOAR 提供的 api，并创建或执行剧本启动对应的自动化流程以达到敏感数据访问，执行命令等相关操作。

该漏洞无需前置用户权限，无需用户交互，攻击成本低。但其利用价值很大程度上取决于 REST API 本身具备哪些功能，同时 SOAR 的执行器一般都运行在沙箱中，想要完成沙箱逃逸入侵到具体的物理机可能还需要其他的漏洞配合。

对此，360CERT 建议广大用户及时将CortexXSOAR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 漏洞详情

2.1 CVE-2021-3044: Cortex XSOAR 未认证 REST API 使用漏洞

CVE: CVE-2021-3044

组件: Cortex XSOAR

漏洞类型: 未认证 REST API 使用

影响: 未认证使用任意 REST API 完成对应操作

简述: 由于 Cortex XSOAR 的认证检验存在缺陷，允许未经认证的攻击者访问 Cortex XSOAR 的 API，并根据 API 所提供的功能创建或执行任意的自动化流程。**该漏洞仅影响具有 active API（活跃 API 秘钥）秘钥的 Cortex XSOAR 配置。**

3 影响版本

产品版本	影响版本
Cortex XSOAR 6.2.0	< 1271065
Cortex XSOAR 6.1.0	>= 1016923 and < 1271064
Cortex XSOAR 6.0.2	不受影响
Cortex XSOAR 6.0.1	不受影响
Cortex XSOAR 6.0.0	不受影响
Cortex XSOAR 5.5.0	不受影响

4 修复建议

4.1 通用修补建议

建议用户根据该影响修复表及时下载安装安全补丁，完成产品的安全更新。

产品版本	安全版本
Cortex XSOAR 6.2.0	>=1271065
Cortex XSOAR 6.1.0	< 1016923 and >= 1271064

4.2 临时修补建议

撤销所有的 active API（活跃 API 秘钥）秘钥可以缓解该漏洞的影响。

具体步骤：

- 在 Cortex XSOAR 中查看所有的 API Key：Settings > Integration > API Keys
- 逐一撤销 API Key
- 利用请求白名单的方式限制 Cortex XSOAR 的请求对象

5 时间线

2021-06-22 Palo Alto 发布漏洞通告

2021-06-23 360CERT 发布通告

6 参考链接

Palo Alto 官方安全通告

A 产品侧解决方案

若想了解更多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 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.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