comware v7安全产品不涉及漏洞CVE-2021-25281、CVE-2021-25282、CVE-2021-25283

漏洞相关 **杨雅伦** 2021-05-14 发表

漏洞相关信息

漏洞编号： CVE-2021-25281、CVE-2021-25282、CVE-2021-25283
漏洞名称： SaltStack漏洞
产品型号及版本： comware v7安全产品

漏洞描述

2021年2月25日，SaltStack发布安全更新，修复了CVE-2021-25281、CVE-2021-25282、CVE-2021-25283三个安全漏洞，攻击者可利用漏洞，实施未授权远程命令执行。受影响的软件版本包括：SaltStack <= 3002.2、SaltStack <= 3001.4、SaltStack <= 3000.6。

CVE-2021-25281: salt-api未校验wheel_async客户端的eauth凭据，受此漏洞影响攻击者可远程运行master上任意wheel模块。

CVE-2021-25282: salt.wheel.pillar_roots.write方法存在目录穿越漏洞。

CVE-2021-25283: 内置Jinja渲染引擎存在SSTI（Server Side Template Injection，服务端模板注入）漏洞。

SaltStack是基于python开发的一套C/S自动化运维工具，能够支持运维管理数万台服务器，主要功能是管理配置文件和远程执行命令，十分强大且易用。 通过部署SaltStack，运维人员可以在成千万台服务器上做到批量执行命令，根据不同业务进行配置集中化管理、分发文件、采集服务器数据、操作系统基础及软件包管理等，SaltStack是运维人员提高工作效率、规范业务配置与操作的利器。

漏洞解决方案

comware平台没有这个软件，不涉及