防火墙是否涉及Splunk Enterprise远程代码执行漏洞（CVE-2022-32158）

漏洞相关 **孔凡安** 2022-06-25 发表

问题描述

防火墙是否涉及Splunk Enterprise远程代码执行漏洞（CVE-2022-32158）

近日，奇安信CERT监测到 Splunk发布Splunk Enterprise远程代码执行漏洞通告，Splunk Enterprise部署服务器9.0之前的版本存在远程代码执行漏洞，允许客户端将转发器捆绑包通过该服务器部署到其他部署客户端。控制了通用转发器端点的攻击者可利用该漏洞在订阅部署服务器的所有其他通用转发器端点上执行任意代码。**鉴于这些漏洞影响范围极大，建议客户尽快做好自查及防护。**

漏洞名称	**Splunk Enterprise 远程代码执行漏洞**		
公开时间	2022-06-15	**更新时间**	2022-06-22
CVE编号	CVE-2022-32158	**其他编号**	QVD-2022-9378
威胁类型	代码执行	**技术类型**	业务逻辑问题
厂商	Splunk	**产品**	Splunk Enterprise
风险等级			
奇安信CERT风险评级		**风险等级**	
高危		**蓝色（一般事件）**	
现时威胁状态			
POC状态	**EXP状态**	**在野利用状态**	**技术细节状态**
未发现	未发现	未发现	未公开
漏洞描述	Splunk Enterprise部署服务器9.0之前的版本存在远程代码执行漏洞，允许客户端将转发器捆绑包通过该服务器部署到其他部署客户端。控制了通用转发器端点的攻击者可利用该漏洞在订阅部署服务器的所有其他通用转发器端点上执行任意代码。		
影响版本	Splunk Enterprise < 9.0		
不受影响版本	Splunk Enterprise >= 9.0		
其他受影响组件	使用部署服务器的Splunk Cloud Platform (SCP)		

风险等级

奇安信 CERT风险评级为：高危

风险等级：蓝色（一般事件）

威胁评估

漏洞名称	Splunk Enterprise 远程代码执行漏洞		
CVE编号	CVE-2022-32158	**其他编号**	QVD-2022-9378
CVSS 3.1评级	高危	**CVSS 3.1分数**	9.0
CVSS向量	**访问途径（AV）**	**攻击复杂度（AC）**	
	网络	高	
	所需权限（PR）	**用户交互（UI）**	
	无	不需要	
	影响范围（S）	**机密性影响（C）**	
	改变	高	
	完整性影响（I）	**可用性影响（A）**	
	高	高	
危害描述	攻击者可以利用该漏洞在目标主机上执行远程代码，完全控制目标主机，读取敏感数据、安装后门等。		

解决方法

不涉及