VCFC如何修复CVE-2020-1938漏洞

VCFC 路康 2021-05-11 发表

漏洞相关信息

漏洞编号： CVE-2020-1938

漏洞名称： ApacheTomcat文件读取/文件包含漏洞

产品型号及版本： VCFC-E2180P13

漏洞描述

ApacheTomcat是由Apache软件基金会属下Jakarta项目开发的Servlet容器，默认情况下，ApacheTomcat会开启AJP连接器,方便与其他Web服务器通过AJP协议进行交互。ApacheTomcat在AJP协议的实现上存在漏洞，导致攻击者可以通过发送恶意的AJP请求，可以读取或者包含Web应用根目录下的任意文件。如果配合文件上传任意格式文件，将可能导致任意代码执行。ApacheTomcat是由Apache软件基金会属下Jakarta项目开发的Servlet容器，默认情况下，ApacheTomcat会开启AJP连接器,方便与其他Web服务器通过AJP协议进行交互。

ApacheTomcat在AJP协议的实现上存在漏洞，导致攻击者可以通过发送恶意的AJP请求，可以读取或者包含Web应用根目录下的任意文件。该漏洞源于Tomcat在接收AJP请求的时候调用org.apache.coyote.ajp.AjpProcessor来处理AJP消息，prepareRequest将AJP里面的内容取出来设置成request对象的Attribute属性，最终借助某些属性进行文件读取。

漏洞解决方案

可以通过修改tomcat配置文件解决

修改如下文件，

vi /opt/sdn/virgo/configuration/tomcat-server.xml

将这行加上注释，然后后台reboot重启控制器即可， 修改完一台控制器后重启那台，等待配置恢复后继续下一台操作