

知 SDN产品关于Apache Tomcat漏洞的整改说明

ADDC解决方案 ADMAN解决方案 刘玉娟 2020-03-07 发表

组网及说明

涉及的SDN产品:

VCFC: 强控E2180P24及之前版本、弱控E2506及之前版本

License server: E1141及之前版本

VNFM2.0&3.0、NFVO所有版本

(DR1000&DR2000、SNA Center、ADWAN均不涉及)

问题描述

Apache Tomcat文件包含漏洞 (CNNVD-202002-1052、CVE-2020-1938) , 成功利用该漏洞的攻击者可以读取 Tomcat所有webapp目录下的任意文件。

过程分析

漏洞详情可参见国家信息安全漏洞库: <http://www.cnnvd.org.cn/web/bulletin/bulletinById.tag?mkid=178>

解决方法

规避措施:

1. 登陆控制器后台找到配置文件, 修改方法如下:

VCFC & VNFM3.0 & NFVO :

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

License Server & VNFM2.0:

/opt/tomcat/apache-tomcat- 7.0.**/conf/server.xml

2. 在配置文件中禁用AJP协议端口, 各产品的端口和内容稍有区别, 以VCFC举例:

```
修改<Connector port="8009" protocol="AJP/1.3" redirectPort="8443"
      maxHttpHeaderSize="8192" />
```

修改为

```
<!-- <Connector port="8009" protocol="AJP/1.3" redirectPort="8443"
      maxHttpHeaderSize="8192" /> -->
```

3. 保存退出后重启控制器, License server只需重启Tomcat服务, HA环境建议先改备机再改主机。

4. VCFC和License server也可以通过升级到不涉及的版本解决。