关于“永恒之蓝”勒索病毒对iMC业务的影响及应对方案的技术公告

寻尚岩 2017-05-13 发表

【产品型号】

H3C iMC APM

H3C iMC ADDC

H3C iMC SecCenter A2000

H3C iMC EIA

H3C iMC SDNAPP ADEIA

【涉及版本】

上述组件所有版本

【问题描述】

5月12日晚，一款名为Wannacry的蠕虫勒索软件袭击全球网络，这被认为是迄今为止最巨大的勒索交费活动，并已影响到上百个国家上千家企业及公共组织。该勒索软件会扫描开放445文件共享端口的Windows机器，对客户业务造成严重影响。根据国家互联网应急中心《关于防范Windows操作系统勒索软件Wannacry的情况通报》，为解决该病毒的影响，需要在网络边界设备、防火墙上阻断对135/137/138/139/445端口的访问。

关闭这些端口会对上述涉及的iMC业务组件在特定场景下产生影响。具体表现为：

1、H3C iMC APM/ DR1000 ADDC/ SecCenter A2000：

H3C iMC APM/ DR1000 ADDC/ SecCenter A2000在监控Windows系统时，监控功能是通过WMI方式实现的，使用的端口为TCP135/445，如果对被监控的Windows服务器关闭135/445端口，会导致H3C iMC APM/ DR1000 ADDC/ SecCenter A2000无法正常监控Window系统。

2、H3C EIA/SDNAPP ADEIA：

iMC配合微软AD服务器进行PEAP Mschapv2认证时需要使用TCP 445端口，关闭微软AD服务器445端口会导致PEAP Mschapv2认证失败，请勿关闭微软AD服务器的445端口，请勿关闭微软AD服务器的445端口。

为解决“永恒之蓝”勒索病毒影响而关闭相关端口会对上述涉及的iMC业务组件在特定应用场景下产生影响。

1、H3C iMC APM/ DR1000 ADDC/ SecCenter A2000：

1) 微软已发布补丁MS17-010修复了该病毒引发的漏洞，请及时对iMC服务器中被监管的Windows服务器安装此补丁。

2) 设置入网防火墙策略，阻止除iMC服务器以外其他IP访问被监管的Windows服务器135/445端口。

3) 为安全起见，请及时对iMC自身所在的Windows服务器安装MS17-010补丁

2、H3C EIA/SDNAPP ADEIA：

1) 微软已发布补丁MS17-010修复了该病毒引发的漏洞，请及时对Windows AD服务器安装此补丁。若要更新其他Windows补丁，请与技术支持中心确认。

2) 设置入网防火墙策略，阻止除iMC服务器以外其他IP访问Windows AD服务器的445端口。

3) 为安全起见，请及时对iMC自身所在的Windows服务器安装MS17-010补丁。