

知 SNA Center关于漏洞CVE-2016-2183整改方法

SNA Center 董婉君 2021-08-23 发表

漏洞相关信息

漏洞编号： CVE-2016-2183

漏洞名称： OpenSSL 信息泄露漏洞

产品型号及版本： SNA Center

漏洞描述

OpenSSL是Openssl团队的一个开源的能够实现安全套接层（SSLv2/v3）和安全传输层（TLSv1）协议的通用加密库。该产品支持多种加密算法，包括对称密码、哈希算法、安全散列算法等。

TLS、SSH和IPSec协议和其它协议及产品中使用的DES和Triple DES密码算法存在信息泄露漏洞。该漏洞源于网络系统或产品在运行过程中存在配置等错误。未授权的攻击者可利用漏洞获取受影响组件敏感信息。

漏洞解决方案

NA Center产品通过添加安全策略解决
新增disable-kubenab安全策略

新增策略

应用

基本设置

名称 *
disable-kubenab

描述

默认动作 *
允许

规则信息

+ 新增 刷新

规则序号	源地址	协议类型	目标端口	动作	操作
1	ANY	TCP	8443	允许	✎ ⌵ ⬆ ⬇
2	ANY	TCP	4443	拒绝	✎ ⌵ ⬆ ⬇

配置如下规则禁用4443端口

新增规则



规则序号

2

源地址

协议类型

TCP

目标端口

4443

动作 *

拒绝

取消

应用

并启用该安全策略

+ 新增 刷新

名称	描述	默认动作	操作
disable-kubenab	--	允许	✎ ⌵ ⬆ ⬇

