# F1000-C8102 DES和Triple DES 信息泄露漏洞

漏洞 聂骋 2021-05-19 发表

## 漏洞相关信息

漏洞编号： CVE-2016-2183
漏洞名称： DES和Triple DES 信息泄露漏洞
产品型号及版本： F1000-C8102

## 漏洞描述

TLS（Transport Layer Security，安全传输层协议）是一套用于在两个通信应用程序之间提供保密性和数据完整性的协议。SSH（全称Secure Shell）是国际互联网工程任务组（IETF）的网络小组（Network Working Group）所制定的一套创建在应用层和传输层基础上的安全协议。IPSec（全称InternetProtocolSecurity）是国际互联网工程任务组（IETF）的IPSec小组建立的一组IP安全协议集。DES和Triple DES都是加密算法。;TLS、SSH和IPSec协议和其它协议及产品中使用的DES和Triple DES密码算法存在安全漏洞。远程攻击者可通过实施生日攻击利用该漏洞获取明文数据。

## 漏洞解决方案

升级到官网最新的E6472P01，并且接口下关闭center-monitor即可。

| 操作 | 命令 | 说明 |
| --- | --- | --- |
| 进入配置视图 | system-view | — |
| 进入以太网接口视图 | interface *name* | — |
| 配置接口管理访问 | allow access {center-monitor\|http\|https\|ping\|telnet\|ssh\|all} | 可选 |