# 二代堡垒机 SSL/TLS协议信息泄露漏洞

漏洞相关 **孔梦龙** 2022-03-15 发表

## 漏洞相关信息

漏洞编号： CVE-2016-2183
漏洞名称： SSL/TLS协议信息泄露漏洞
产品型号及版本： 不区分

## 漏洞描述

TLS是安全传输层协议，用于在两个通信应用程序之间提供保密性和数据完整性。 TLS, SSH, IPSec协商及其他产品中使用的DES及Triple DES密码存在大约四十亿块的生日界，这可使远程攻击者通过Sweet32攻击，获取纯文本数据。 <*来源：Karthik Bhargavan Gaetan Leurent 链接：https://www.openssl.org/news/secadv/20160922.txt *>

## 漏洞解决方案

老平台最新E6104P04解决，可以升级E6104P05。老平台的上限版本是6104P05，不支持升级611X以上；

新平台原则上不涉及，建议升级最新版本