数据库审计D2050-G 【原理扫描】SSL/TLS协议信息泄露漏洞(CVE-2016-2183)解决办法

数据库审计 吴超 2021-07-01 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： D2050-G

漏洞描述

SSL/TLS协议信息泄露漏洞(CVE-2016-2183)漏洞： SSL全称是Secure Sockets Layer，安全套接字层，它是由网景公司（Netscape）设计的主要用于Web的安全传输协议，目的是为网络通信提供机密性、认证性及数据完整性保障。如今，SSL已经成为互联网保密通信的工业标准。SSL最初的几个版本（SSL 1.0、SSL2.0、SSL 3.0）由网景公司设计和维护，从3.1版本开始，SSL协议由因特网工程任务小组（IETF）正式接管，并更名为TLS（Transport Layer Security），发展至今已有TLS 1.0、TLS1.1、TLS1.2，TLS1.3这几个版本。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。 风险级别：低 该漏洞又称为SWEET32（https://sweet32.info）是对较旧的分组密码算法的攻击，它使用64位的块大小，缓解SWEET32攻击OpenSSL 1.0.1和OpenSSL 1.0.2中基于DES密码套件从“高”密码字符串组移至“中”；但OpenSSL 1.1.0发布时自带这些，默认情况下禁用密码套件。该问题在新的openssl版本中已解决。

漏洞解决方案

升级至E6204P02及以后的版本解决。