网络安全预警通报

2024年第1期

网络中心　　2024年3月26日

【预警类型】 **高危预警**

【预警内容】

关于麒麟系统 V10 存在 openssl 漏洞的安全公告

一、漏洞概述

2024 年 3 月 11 日，麒麟官方公布了一系列 openssl 的安全漏洞，包括 CVE-2022-1343、CVE-2022-1292、CVE-2022-1434 和 CVE-2022-1473。该系列安全漏洞会对麒麟部分系统带来安全隐患，建议及时升级系统，减少安全风险带来的危害。

二、漏洞详情

OpenSSL 是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。

CVE-2022-1343：OpenSSl 存在信任管理问题漏洞，该漏洞源于 OCSP_basic_verify 函数用于验证签名者证书，在使用标志

OCSP_NOCHECKS 的情况下，即使在响应签名证书无法验证的情况下，也会验证成功。

CVE-2022-1292：OpenSSL 存在操作系统命令注入漏洞，该漏洞源于 c_rehash 脚本未正确清理 shell 元字符导致命令注入。攻击者利用该漏洞执行任意命令。

CVE-2022-1434：OpenSSL 存在安全漏洞，该漏洞源于 RC4-MD5 密码套件错误地将 AAD 数据用作 MAC 密钥。这使得 MAC 密钥可以轻松预测。攻击者可以利用该漏洞通过执行中间人攻击来修改从一个端点发送到 OpenSSL3.0 接收者的数据，从而使修改后的数据仍能通过 MAC 完整性检查。

CVE-2022-1473：OpenSSL 存在安全漏洞，该漏洞源于清空哈希表的 OPENSSL_LH_flush()函数包含一个错误，该错误会破坏已删除的哈希表条目占用的内存的重用。攻击者利用该漏洞可以实现拒绝服务攻击。

漏洞影响范围：

银河麒麟桌面操作系统 V10 SP1

x86_64 架构：libssl1.1、openssl

arm64 架构：libssl1.1、openssl

mips64el 架构：libssl1.1、openssl

loongarch64 架构：libssl1.1、openssl

三、处置建议

1、执行更新命令进行升级：

$sudo apt update

$sudo apt install openssl

2、下载软件包进行升级安装：

通过软件包地址下载软件包，使用软件包升级命令根据受影响的软件包列表升级相关的组件包。

$sudo dpkg -i /Path1/Package1/Path2/Package2/Path3/Package3…

注：Path 指软件包下载到本地的路径，Package 指下载的软件包名称，多个软件包则以空格分开。

参考链接：

https://kylinos.cn/support/loophole/patch/5400.html