网络安全预警通报

2024 年第 2 期 （总第 45 期）

西安交通大学网络信息中心 2024 年 4 月 1 日

【预警类型】 **高危预警**

【预警内容】

关于 XZ-Utils 5.6.0/5.6.1 版本后门风险的安全公告

一、漏洞概述

2024 年 3 月 29 日，安全社区披露其存在 XZ-Utils 5.6.0-5.6.1 版本后门风险，漏洞编号：CVE-2024-3094。攻击者可能利用该漏洞在受影响的系统上绕过 SSH 的认证获得未授权访问权限，执行任意代码。。

二、漏洞详情

XZ-Utils 是 Linux、Unix 等 POSIX 兼容系统中广泛用于处理.xz 文件的套件，包含 liblzma、xz 等组件，已集成在 debian、ubuntu、centos 等发行版仓库中。2024 年 3 月 29 日，安全社区披露其存在 CVE-2024-3094 XZ-Utils 5.6.0-5.6.1 版本后门风险。该后门存在于 XZ-Utils 的 5.6.0 和 5.6.1 版本中，由于 SSH 底层依赖了 liblzma 等，攻击者可能利用这一漏洞在受影响的系统上绕过 SSH 的认证获得未授权访问权限，执行任意代码。

漏洞影响范围：

5.6.0

5.6.1

注：企业主流使用的 Linux 发行版（例如 Red Hat、CentOS、Debian、Ubuntu）的 Stable 稳定版未合并存在后门的版本，因此不受影响。建议客户根据实际情况进行排查。

三、处置建议

1、可使用云安全中心-主机资产-中间件功能查询进程所使用依赖的 liblzma 版本，或者手动运行 xz-V 或 xz-version 获取系统安装的 xz/liblzma 版本。

2、若使用了受影响版本 xz/liblzma 的操作系统（Fedora 41、Debian sid 测试版等）建议更新至安全版本。具体详情可在查询：https://repology.org/project/xz/versions

参考链接：

https://avd.aliyun.com/detail?id=AVD-2024-3094