网络安全预警通报

2023 年第 6 期 （总第 43 期）

西安交通大学网络信息中心 2023 年 12 月 22 日

【预警类型】 **高危预警**

【预警内容】

关于蓝牙协议存在中间人攻击漏洞的安全公告

一、漏洞概述

2023 年 12 月 20 日，国家信息安全漏洞共享平台（CNVD）收录了蓝牙协议中间人攻击漏洞（CNVD-2023-98846，对应 CVE-2023-24023）。攻击者利用漏洞通过欺骗性的配对或绑定设备强制使用较短的加密密钥长度，破坏蓝牙设备会话的安全验证机制。目前，漏洞技术原理已公开，CNVD 建议受漏洞影响的设备厂商和用户加强安全防范措施。

二、漏洞详情

蓝牙（Bluetooth）是一种支持设备短距离通信的无线电通信协议，目前已成为全球通用的开放性技术规范，广泛应用于个人终端、车载娱乐、工业生产和医药医疗领域。蓝牙设备的有效传输距离一般小于 10 米，其通信质量易受障碍物的影响。法国 EURECOM 安全研究员兼助理教授

Daniele Antonioli发现了蓝牙BR/EDR设备的安全连接配对和安全简单配对的核心规范存在安全漏洞。位于目标设备有效蓝牙传输距离内的攻击者利用上述漏洞，通过捕获和伪造蓝牙会话数据包，可对目标会话发起中间人攻击（BLUFFS）。BLUFFS 攻击能够破坏蓝牙配对设备的会话身份验证机制，通过使用欺骗性的配对或绑定设备强制使用较短的加密密钥长度，继而破坏蓝牙通信会话的保密性和完整性。

漏洞影响范围：

蓝牙协议核心规范，版本范围为 4.2（2014 年 12 月发布）至 5.4（2023 年 2 月发布）。

三、处置建议

1、CNVD 建议蓝牙设备厂商将蓝牙设备的默认设置修改为安全连接模式，以确保密钥强度；

2、建议蓝牙设备用户加强安全防范措施，开启蓝牙连接时注意周围的可疑设备，同时使用高强度的蓝牙通信密钥。

参考链接：

https://www.bluetooth.com/learn-about-bluetooth/key-attributes/bluetooth-security/bluffs-vulnerability/