Smartbi 商业智能软件破解用户密码和 DB2 绕过判断执行命令漏洞通告

■ **通告编号**	**NS-2023-00**	■ 发布日期	**2023-07-28**
■ **漏洞危害**	**攻击者利用该漏洞后可获取用户访问权限，进一步入侵获得系统权限或执行命令**		
■ **TAG**	Smartbi、破解用户密码、DB2 绕过判断执行命令		

一. 漏洞概述

近日，绿盟科技 CERT 监测到 Smartbi 官方修复了破解用户密码和 DB2 绕过判断执行命令漏洞。Smartbi 在某种特定情况下存在破解用户密码和特定情况下 DB2 绕过判断执行命令问题，攻击者成功利用该漏洞后可获取用户访问权限，进一步入侵获得系统权限或执行命令，进而对目标系统造成破坏或篡改窃取敏感信息。请受影响的用户尽快采取措施进行防护。

Smartbi 是广州思迈特软件有限公司旗下的商业智能 BI 和数据分析品牌。Smartbi 致力于为企业客户提供一站式商业智能解决方案。

参考链接：

https://mp.weixin.qq.com/s/nM7pyoubjQn3Qqzq2LPLag

二. 影响范围

受影响范围

- Smartbi >= V6

三. 漏洞防护

3.1 官方升级

目前官方已发布补丁包修复此漏洞，请使用 Smartbi V6 及其以上版本产品的用户及时下载最新补丁包进行防护，参考链接：

https://www.smartbi.com.cn/patchinfo

安全补丁更新具体操作请参考：https://wiki.smartbi.com.cn/pages/viewpage.action?pageId=50692623

注：其中“某种特定情况下破解用户密码”漏洞需要配合系统设置，修复方案详见：https://wiki.smartbi.com.cn/pages/viewpage.action?pageId=114996930

声明

本安全公告仅用来描述可能存在的安全问题，绿盟科技不为此安全公告提供任何保证或承诺。由于传播、利用此安全公告所提供的信息而造成的任何直接或者间接的后果及损失，均由使用者本人负责，绿盟科技以及安全公告作者不为此承担任何责任。

绿盟科技拥有对此安全公告的修改和解释权。如欲转载或传播此安全公告，必须保证此安全公告的完整性，包括版权声明等全部内容。未经绿盟科技允许，不得任意修改或者增减此安全公告内容，不得以任何方式将其用于商业目的。