

安全补丁

Smartbi添加了一种安全补丁机制，能够在不更新war包的前提下，只更新安全补丁。

该安全补丁可以修复一些系统漏洞，避免发生由于漏洞引起的安全事故。

- 更新安全补丁
 - 判断系统版本
 - 安装补丁工具包
 - 更新补丁工具包
 - 更新安全补丁文件
 - 在线更新
 - 手动更新
 - 集群环境更新补丁
- 说明事项
 - 授权IP地址访问config和monitor页面
 - 限制config/chooser.jsp文件访问路径

在Smartbi中安装安全补丁涉及以下两个文件：

补丁工具包：补丁工具包是用来上传安全补丁文件的载体，通过此工具包可在Smartbi服务器上上传安全补丁文件。（当前补丁工具包最新版本为1.0）

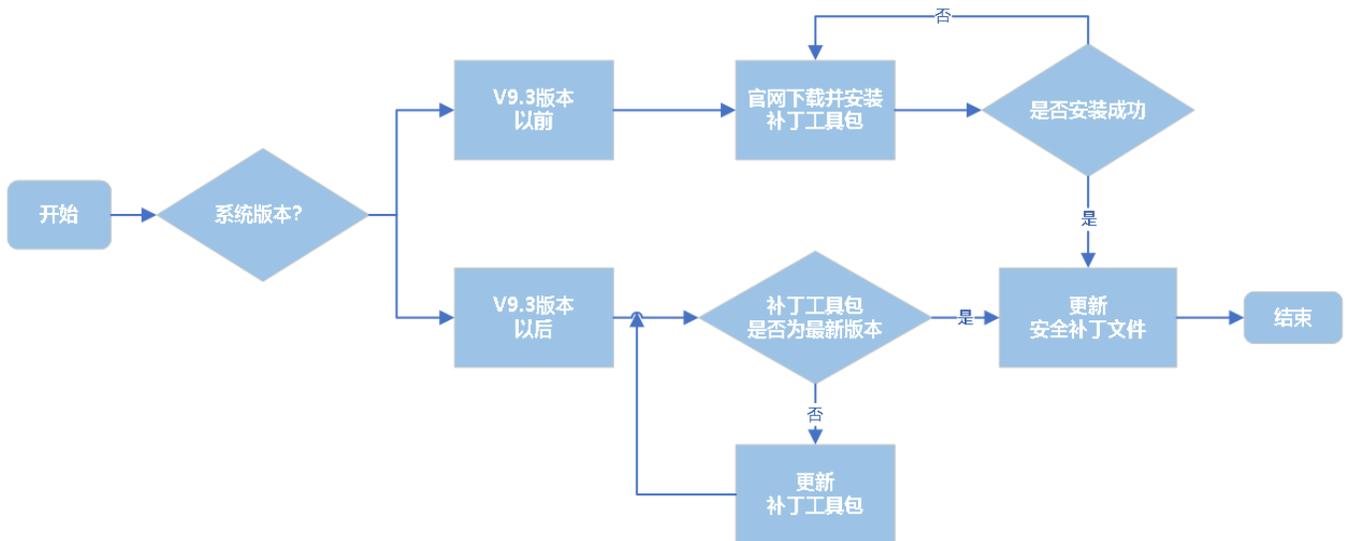
安全补丁文件：安全补丁文件中包含了目前我们检测修复的安全漏洞程序。Smartbi会不定期在官网更新安全补丁文件，用户可下载此文件，并直接更新到Smartbi服务器中，已解决已知的一些安全漏洞。

根据实际情况，在官网下载补丁工具包或安全补丁文件，官网如图：<https://www.smartbi.com.cn/patchinfo>

本文适用V10版本，其他版本请参考：

系统版本	详细信息
V6	关于V6版本更新安全补丁，详情请参考 安全补丁 。
V7	关于V7版本更新安全补丁，详情请参考 系统监控-安全补丁 。
V8	关于V8版本更新安全补丁，详情请参考 系统监控-安全补丁 。
V9	关于V9版本更新安全补丁，详情请参考 系统监控-安全补丁 。

更新安全补丁流程如下：



更新安全补丁

判断系统版本

在系统的右上角上点击 **用户名** > **关于** ，查看系统版本，再进行下一步操作：

- 如果当前系统版本为V9.3以前的版本，则表明系统没有默认带有补丁工具包，需要先到官网安装补丁工具包，具体请参考 [安装补丁工具包](#)。
- 如果当前系统版本为V9.3及以后的版本，则表明系统默认带有补丁工具包，需要检查补丁工具包版本是否需要更新，具体请参考 [更新补丁工具包](#) 。

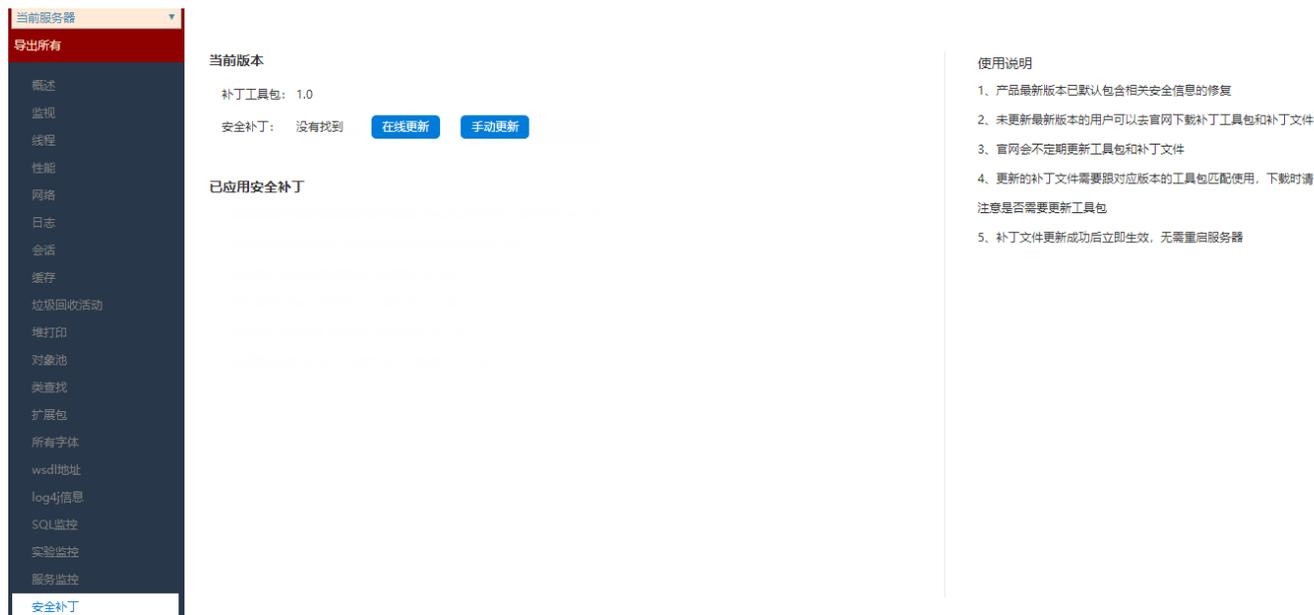


安装补丁工具包

前提：当前系统版本为V9.3以前的版本，且未安装过安全补丁。

具体操作如下：

- 1、去官网根据版本下载最新的补丁工具包。下载地址：[Smartbi安全补丁包下载](#)。
- 2、参考文档 [扩展包部署](#) ，将获取到的安装补丁工具包部署到Smartbi应用服务器上。
- 3、完成部署后，重启Smartbi应用服务器，验证是否安装成功。可在系统监控面板查看是否补丁工具包安装成功：



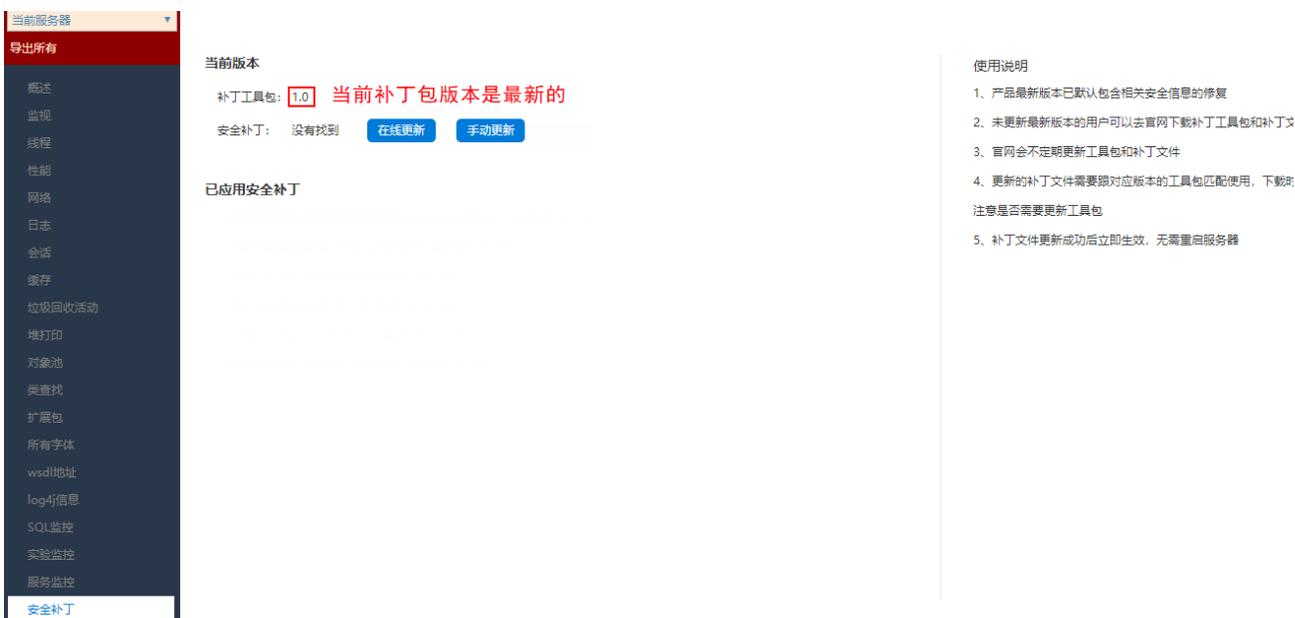
安装完补丁工具包后，补丁工具包版本已是最新的，接下来 [更新安全补丁文件](#) 即可。

更新补丁工具包

前提：当前系统版本为V9.3及以后的版本，或曾经安装过补丁工具包但不确定补丁工具包是否为最新。

具体操作如下：

- 1、打开系统监控面板。查看已安装的补丁工具包，再与官网上最新的补丁工具包对比，判断当前补丁工具包的版本是否为最新。
 - 如果是最新，则只需更新安全补丁文件。详情请参考 [更新安全补丁文件](#) 。
 - 如果不是最新，则需先更新补丁工具包，之后更新安全补丁文件。具体请看下个步骤。



- 2、去官网根据版本下载最新的补丁工具包。下载地址：[Smartbi安全补丁包下载](#)。
- 3、参考文档 [扩展包部署](#) ，将获取到的安装补丁工具包部署到Smartbi应用服务器上。
- 4、完成部署后，重启Smartbi应用服务器，再次打开系统监控界面，查看补丁工具包的版本信息，验证是否更新成功。

更新安全补丁文件

前提：安全补丁文件需要更新，且当前补丁工具包的版本为最新。

更新安全补丁文件，可选择 **手动更新** 与 **在线更新** 两种方式。



区别：

- 1、“在线更新”功能要求当前系统环境能正常访问外网，否则会提示更新失败。
- 2、“手动更新”功能对网络环境无要求，只需在官网下载最新的安全补丁文件，通过上传补丁文件更新。

在线更新

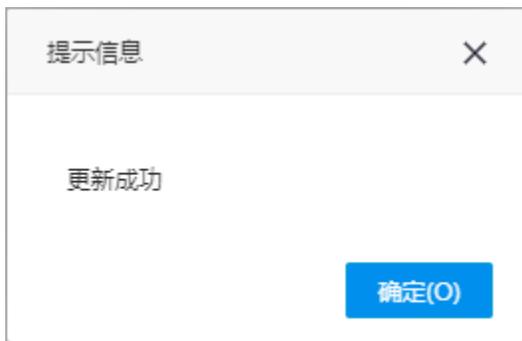
1、打开系统监控面板，进入“安全补丁”界面，点击 **在线更新** 按钮，系统会到官网上自动获取最新的安全补丁文件进行更新。



使用说明

- 1、产品最新版本已默认包含相关安全信息的修复
- 2、未更新最新版本的用户可以去官网下载补丁工具包和补丁文件
- 3、官网会不定期更新工具包和补丁文件
- 4、更新的补丁文件需要跟对应版本的工具包匹配使用，下载时请注意是否需要更新工具包
- 5、补丁文件更新成功后立即生效，无需重启服务器

2、提示“更新成功”，则更新安全补丁文件完成。



手动更新

- 1、先从官网下载最新的补丁更新文件，下载地址：[Smartbi安全补丁包下载](#)。
- 2、打开系统监控面板，进入“安全补丁”界面，点击 **手动更新** 按钮，选择刚下载的安全补丁文件并上传。



- 3、提示“更新成功”，则更新安全补丁文件完成。



集群环境更新补丁

以上补丁更新都默认是在“当前服务器”中更新，在集群环境下，支持用户选择更新的服务器：

安全补丁 升级补丁

选择更新的服务器

当前版本

补丁工具包：1.0

安全补丁： 2021-07-16 18:25:00 [在线更新](#) [手动更新](#)

已应用安全补丁

- 修复了脚本注入漏洞 (Patch.20210824 @2021-08-24)
- 修复了产品登录验证的漏洞 (Patch.20210716 @2021-07-16)
- 修复可任意上传文件的漏洞 (Patch.20210428 @2021-04-28)
- 限制配置界面及管理页面的访问地址 (Patch.20210318 @2021-03-18)
- config界面的文件路径增加访问限制 (Patch.20201014 @2020-10-14)
- 修复补丁包日期显示异常问题 (Patch.20200603 @2020-06-03)
- 限制配置界面及管理页面的访问地址 (Patch.20200414 @2020-04-14)
- 去低级登录配置界面 (Patch.20200325 @2020-03-25)

使用说明

- 产品最新版本已默认包含相关安全信息的修复
- 未更新最新版本的用户可以去官网下载补丁工具包和补丁文件
- 官网会不定期更新工具包和补丁文件
- 更新的补丁文件需要跟对应版本的工具包匹配使用，下载时请注意是否需要更新工具包
- 补丁文件更新成功后立即生效，无需重启服务器

可供选择的服务器通过 **设置** 功能进行设置：

设置

添加服务器

服务器名称	地址*	用户名*	密码	操作
Server1	http://10.10.111.32:8094/smartbi	admin	*****	🗑️

[确定\(O\)](#) [取消\(C\)](#)

说明

- 产品最新版本已默认包含相关安全信息的修复
- 未更新最新版本的用户可以去官网下载补丁工具包和补丁文件
- 官网会不定期更新工具包和补丁文件
- 更新的补丁文件需要跟对应版本的工具包匹配使用，下载时请注意是否需要更新工具包
- 补丁文件更新成功后立即生效，无需重启服务器

激活 Windows
转到设置以激活 Windows。

说明事项

授权IP地址访问config和monitor页面

如果访问smartbi的config和monitor配置页面时，提示“未授权的IP地址；或访问其他页面报错，如：调试工具集、地图编辑器报：”该页面需要授权IP地址才能访问，请联系管理员添加”。

← → ↻ ⓘ 不安全 | 10.10.202.17:18600/smartbi/vision/config.jsp

未授权的IP地址 请修改smartbi.properties授权

需要找到Smartbi安装目录下的smartbi.properties文件配置你需要允许的IP。

ⓘ 可以使用英文逗号分隔设置多个IP属性，例如smartbi.allowedConfigIps=10.10.23.11,10.10.201.1-10.10.201.254,10.10.202.0/24

每个属性的配置如下：

类别	方法	示例
允许所有IP	*号代表全部IP。 注：这里不支持10.10.202.*	smartbi.allowedConfigIps=*
精确指定某个ip	直接设置对应的ip地址即可。	smartbi.allowedConfigIps=10.10.101.11
指定多个ip地址	各个ip地址以英文逗号分隔。	smartbi.allowedConfigIps=10.10.101.11,10.10.101.21,10.10.101.31
指定某个ip段地址	指定ip段地址区间，中间用减号(-)连接。	smartbi.allowedConfigIps=10.10.101.0-10.10.101.255
指定ip支持标准的掩码	使用 标准CIDR 格式。计算方法可参考： 计算方法	smartbi.allowedConfigIps=10.10.23.0/24

注意：

- 1、修改后只需刷新页面即可，无需重启服务器。
- 2、allowedConfigIps这个属性控制的是config界面；如果控制的是monitor界面，对应的属性是allowedMonitorIps。
- 3、“smartbi.”这个前缀是上下方路径。如果项目不是使用/smartbi/vision访问，而是/smartbiNew/vision/index.jsp这样，则前缀应当是“smartbiNew.”，即smartbiNew.allowedConfigIps。
- 4、如果服务器为Linux，可以将configip.sh上传到smartbi.properties所在目录，并通过 `chmod 755 configip.sh` 修改为可执行，再运行 `./configip.sh` 通过命令行修改。

命令行修改工具：[configip.sh](#)

- 5、服务器所在的机器ip是不限制的。

限制config/chooser.jsp文件访问路径

前提：产品的补丁工具包和安全补丁文件为最新版本（2020-10-14及之后的日期）。

在 [系统运维](#)>[系统选项](#)>[高级设置](#) 中，设置JSP_CHOOSER_ROOT_PATH设置项可限制config/chooser.jsp页面文件访问路径，值为限制用户可选的最大可选择根目录。

```

224
225 ## 移动端URL控件缩放方式
226 ## 备选值: DEFAULT=默认, FORCE_SCALE=强制缩放至屏幕实际大小
227 ## 初始值(默认)
228 ## MOBILE_URL_RESOURCE_SCALE=DEFAULT
229
230 ## 回写数据大小限制
231 ## 初始值( 1400~1500 )
232 ## SSR_WRITEBACK_DATA_LIMIT=1400~1500
233
234 # SmartbiMpp
235
236 ## 插入数据时自动处理NULL值
237 ## 备选值: true=是, false=否
238 ## 初始值( 否 )
239 ## CLICK_HOUSE_AOTU_CONVERT_NULL=false
240
241 ## 初始值( 5 )
242 ## BACKUP_TAB_RETAIN_NUM=5
243
244 SHOW_APP_PUBLISH_REF=true
245
246 SPREAD_SHEET_REPORT_ALLOW_WRITEBACK=true
247
248 JSP_CHOOSER_ROOT_PATH=/tomcat/smartbiconfig
    
```

格式化代码(F) 帮助(H)

保存(S) 关闭(C)



如果用户手动修改config.jsp/chooser.jsp 中的存放目录, 会导致存放目录大于根目录, 且系统会提示“超出最大可选择根目录范围”。