

Weaver Software

上海浦东耀华支路39弄9号泛微软件大厦

邮政编码：200127

电话：+86 21 50942228

传真：+86 21 50942278

**Ecology系统安全安装说明**

**Submitted By Weaver**

**设计说明书**

文档版本控制

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **文档简要信息：** | | | | | | | |
| 文档主题(Title) | | | | Ecology系统安全配置说明 | | | |
| 作者(Author) | | | | 柳炉 | | | |
| 审批者 (To Be Approved By) | | | |  | | | |
| 说明 (Comments) | | | | Ecology系统安全配置说明 | | | |
| 文件名称(File Name) | | | |  | | | |
| **文档版本历史：** | | | | | | | |
| 序号 | 日期 | 版本 | 变更说明 | | 修改人 | 审批人 | 注释 |
|  | 2015/03/20 | 1 | 新建 | | 柳炉 |  |  |
|  | 2015/03/22 | 2 | 针对使用非UTF-8编码开发的页面配置 | | 柳炉 |  |  |
|  | 2015/03/30 | 3 | 增加webservice安全验证 | | 柳炉 |  |  |
|  | 2016/08/08 | 1 | 初始版本 | | 柳炉 |  |  |
|  | 2016/08/12 | 2 | 修正截图内容 | | 柳炉 |  |  |
|  | 2016/09/13 | 3 | 修改 | | 柳炉 |  |  |
|  | 2016/9/23 | 4 | 修改 | | 柳炉 |  |  |
|  | 2018/11/21 | 5 | 新增必须开启的防御功能 | | 柳炉 |  |  |

**目录**

[1 引言 4](#_Toc530587345)

[1.1 编写目的 4](#_Toc530587346)

[1.2 安全包升级步骤 4](#_Toc530587347)

[1.3 必须做好的安全加固工作 9](#_Toc530587348)

[1.3.1 Webservice安全防护规则 9](#_Toc530587349)

[1.3.2 Windows服务器安全加固 9](#_Toc530587350)

[1.3.3 Linux系统也不要开放22、23等远程端口到公网 9](#_Toc530587351)

[1.3.4 数据库加固 9](#_Toc530587352)

[1.3.5 仅开放必须开放外网的端口，如果需开放外网服务，默认端口情况下，建议只开启以下端口（如果端口有变更，请根据实际情况调整）： 9](#_Toc530587353)

[1.3.6 应用系统账户口令策略配置 10](#_Toc530587354)

[1.3.7 建议对重要数据（如附件、数据库等）进行定期脱机备份。 10](#_Toc530587355)

# 引言

## 编写目的

本文档主要描述了Ecology系统安全补丁如何进行安装部署。

## 安全包升级步骤

**本安全包适用于Ecology5.0及以上版本。Ecology5.0以下版本不适用。**

1. 从官网上<http://www.weaver.com.cn/cs/securityDownload.html> 上下载最新的安全补丁（Ecology安全补丁），解压后会得到一个ecology文件夹；
2. 停止OA服务，将解压后得到的ecology文件夹覆盖服务器上的ecology文件夹；
3. 重启OA服务，用sysadmin登录系统，访问[http://](http://贵司OA访问地址/security/server.jsp)**[贵司OA访问地址/security/server.jsp](http://贵司OA访问地址/security/server.jsp)**

**如果看到如下图所示的页面，则表示安全补丁安装成功；否则，请检查安全补丁覆盖位置是否正确，重新覆盖安全补丁：**

|  |
| --- |
|  |
| **加入安全保障计划后，泛微会自动检测贵方系统的安全状况，如果发现系统有漏洞，会及时报告并修复漏洞，保障系统处于安全的状态。**  **如果选择加入安全保障计划，泛微会自动收集客户名称、系统版本、安全补丁信息，加密后安全地传输到泛微安全服务器上，以便我们能够准确掌握贵方系统的安全状况，如果发现有问题，会主动联系贵方协助处理，共同保障系统的安全运行。**  **以下文字是根据服务器能否连外网动态输出的，只有服务器不能连外网才会输出这行信息：**  **检测到贵方OA服务器无法联通外网，所以即使选择加入安全保障计划，也无法为您提供安全补丁自动修复功能！** |

1. 点击【上报系统安全补丁安装情况至泛微安全服务器】按钮，将数据上报到泛微安全服务器，该上报数据用于通知泛微安全部门已经正确打上安全包了，收集的数据仅限于**客户名称、系统版本、安全补丁；**

**出现以下截图表明数据正常上报：**

|  |
| --- |
|  |

|  |
| --- |
| 由于服务器采用了https证书方式，所以上报数据时浏览器会识别证书，请按照以下步骤实现数据的上报：  4.1 点击【上报系统安全补丁安装情况至泛微安全服务器】按钮，可能弹出以下界面：  Google浏览器：  图一：弹出确认框，请点击【高级】  图二：点击【继续前往update.e-cology.cn(不安全)】连接  图三：数据上报成功  IE浏览器：  图一：弹出确认框，点击【继续浏览此网站（不推荐）】链接  图二：数据上报成功界面 |

1. 至此，安全补丁成功安装。
2. 检测安全包是否生效的方法

|  |
| --- |
| 1、用sysadmin登录系统，访问:/security/monitor/Monitor.jsp;  2、查看【环境信息】tab页，可以看到当前安全包版本；  3、在【安全概要】tab页，可以看到安全包是否生效；  4、如果显示为未开启，在【安全体检】里面点击【检测】，检测后会弹出【修复】按钮，点击【修复】；  5、修复完成后会弹出 具体的修复步骤（主要就是替换文件），按照修复步骤操作即可  6、如果按上面5步修复完成后仍显示未开启，请在【安全开启详情】tab页的第一项点击【开启】。  7、如果仍显示为未开启，则删除/ecology/WEB-INF/weaver\_security\_config.xml 文件，重启OA或者在【安全开启详情】界面点击【刷新】按钮 |

## 必须做好的安全加固工作

### Webservice安全防护规则

开启方式：修改/ecology/WEB-INF/weaver\_security\_config.xml，将<enable-service-check>改为true，或者在</root>上方新增<enable-service-check>true</enable-service-check>这行代码。

开启后，请参考《webservice白名单防御配置说明.docx》进行白名单配置。

### Windows服务器安全加固

* 必须关闭windows外网远程桌面，防止暴力破解，导致服务器中毒，可以用teamview等第三方工具代替，或者使用跳板机进行二次远程操作；
* 必须将administrator重命名其他名字，防范工具自动化暴力破解，具体方法参考如下：

https://jingyan.baidu.com/article/4dc408488b2187c8d946f1b2.html

### Linux系统也不要开放22、23等远程端口到公网

### 数据库加固

* 数据库服务器严禁开放外网访问，尤其是数据库服务端口如1433、1521、3306等

### 仅开放必须开放外网的端口，如果需开放外网服务，默认端口情况下，建议只开启以下端口（如果端口有变更，请根据实际情况调整）：

|  |  |  |
| --- | --- | --- |
| **产品** | **开放端口（默认端口）** | **备注** |
| **Ecology** | **80** | **PC端访问端口** |
| **EMobile** | **89** | **EMobile移动端访问端口** |
| **E-bridge** | **8088** | **云桥开放端口** |
| **E-message** | **5222,7070** | **Emessage需开放端口**  **9090属于后台管理，不建议开放外网访问。** |

### 应用系统账户口令策略配置



### 建议对重要数据（如附件、数据库等）进行定期脱机备份。