

编号：MSCTC-GFJ-08

信息技术

网站恢复产品安全检验规范

公安部计算机信息系统安全产品质量监督检验中心

第一版 第0次修订
2003年11月01日颁布

2003年12月01日实施

前 言

为了规范全国网站恢复产品的开发与应用，保障公共信息网络安全，根据公安部公共信息网络安全监察局的要求，本规范对网站恢复产品提出了安全功能要求和保证要求，作为对其进行检测的依据。

本规范由中华人民共和国公安部公共信息网络安全监察局提出。

本规范起草单位：公安部计算机信息系统安全产品质量监督检验中心。

公安部计算机信息系统安全产品质量监督检验中心负责对本规范的解释、提升和更改。

信息技术网站恢复产品安全检验规范

1 范围

本规范规定了网站恢复产品的安全功能要求和技术要求。

本规范适用于网站恢复产品的生产及安全功能检测。

2 术语和定义

2.1 网站恢复 website recovery

网站恢复产品是一种对网页内容的未授权更改准实时地进行自动恢复的软件。

3 网站恢复产品的安全功能要求

3.1 网页文件自动恢复功能

网站恢复产品能对受保护静态网页文件的未授权更改进行识别,并能用备份文件进行自动恢复。即:

- a) 网页文件未授权增加的恢复;
- b) 网页文件未授权删除的恢复;
- c) 网页文件未授权修改(包括文件属性修改、重命名、移动等)的恢复。

3.2 网页目录自动恢复功能

网站恢复产品能识别对受保护网页目录的未授权破坏进行识别,并能用备份目录进行自动恢复。即:

- a) 网页目录未授权增加的恢复;
- b) 网页目录未授权删除的恢复;
- c) 网页目录未授权修改(包括目录属性修改、重命名、移动等)的恢复。

3.3 管理功能

3.3.1 管理员身份鉴别

网站恢复产品应保证只有授权管理员能使用产品的管理功能。对授权管理员应进行身份鉴别。

3.3.2 管理员权限

网站恢复产品应保证授权管理员有下列权限:

- a) 管理员属性修改（更改密码等）；
- b) 启动、关闭监控保护服务；
- c) 增加或撤消对所有受保护目录的监控；
- d) 授权合法用户对网页内容进行合法更新。

3.3.3 监控目录/文件管理

3.3.3.1 用户可增加或撤消其相应的被监控的目录/文件；

3.3.3.2 若采用定期扫描的监测机制，则对监控目录/文件遭受未经授权更改的监测时间间隔，用户可自行设置。

3.3.4 备份文件的安全存储及保密传输

3.3.4.1 仅管理员可指定备份端，用户可备份指定文件及目录到备份端；

3.3.4.2 备份端应对登录用户进行身份鉴别，实现备份文件在备份端的安全存储；

3.3.4.3 用备份文件对受保护网页文件的未经授权更改进行恢复时，备份文件应保密传输；

3.3.4.4 应提供网页内容合法更新后的及时备份。

3.3.5 产品自身安全性

应能抵御已知手段攻击，保证其正常运行不受影响。

3.3.6 远程管理的安全性

若提供远程管理功能，应对远程管理的登录信息及会话保密传输。

3.4 报警功能

3.4.1 应对以下事件实时报警：

- a) 对受保护网页文件的未经授权增、删、改的报警；
- b) 对受保护网页目录及属性的未经授权增、删、改的报警；
- c) 对监控保护进程异常关闭的报警。

3.4.2 报警信息的数据格式：

报警信息数据项的内部数据结构定义可参考如下：

序号	名称	类型	长度
1	事件发生日期	字符	8
2	事件发生时间	字符	6
3	事件类型	字符	30
4	备注	字符	100

注：若事件为 3.4.1 a)、b)，则应在备注中指出受破坏文件或目录的位置。

3.4.3 报警方式

应提供适当的报警方式（例如：E_mail 报警）

3.5 审计日志功能

3.5.1 可审计事件：

- a) 对受保护网页文件进行增、删、改和恢复的日志；
- b) 对受保护网页目录进行增、删、改和恢复的日志；
- c) 监控保护服务的开启和关闭的日志。

3.5.2 审计信息的数据格式：

审计信息数据项的内部数据结构定义可参考如下：

序号	名称	类型	长度
1	事件发生日期	字符	8
2	事件发生时间	字符	6
3	事件类型	字符	30
4	备注	字符	100

注：若事件为 3.4.1 a)、b)，则应在备注中指出受破坏文件或目录的位置。

3.5.3 审计跟踪管理

管理员应能创建、存档、删除和清空审计记录。

3.5.4 可理解的格式

该类产品应使存储于永久性审计记录中的所有审计数据为人所理解。

4 网站恢复产品的保证要求

4.1 交付和运行

4.1.1 交付过程

4.1.1.1 开发者行为元素：

- a) 开发者应将把网站恢复产品及其部分交付给用户的程序文档化；
- b) 开发者应使用交付程序。

4.1.1.2 证据元素的内容和表示

交付文档应描述，在给用户方分配网站恢复产品的版本时，用以维护安全所必需的所有程序。

4.1.2 安装、生成和启动程序

4.1.2.1 开发者行为元素

开发者应将网站恢复产品安全地安装、生成和启动所必需的程序文档化。

4.1.2.2 证据元素的内容和表示

文档应描述网站恢复产品安全地安装、生成和启动所必要的步骤。

4.2 指导性文档

4.2.1 管理员指南

4.2.1.1 开发者行为元素

开发者应当提供针对系统管理员的管理员指南。

4.2.1.2 证据的内容和形式元素：

- a) 管理员指南应当描述网站恢复产品管理员可使用的管理功能和接口；
- b) 管理员指南应当描述如何以安全的方式管理网站恢复产品；
- c) 管理员指南应当包含在安全处理环境中必须进行控制的功能和权限的警告；
- d) 管理员指南应当描述所有与网站恢复产品的安全运行有关的用户行为的假设；
- e) 管理员指南应当描述所有受管理员控制的安全参数，合适时，应指明安全值；
- f) 管理员指南应当描述每一种与需要执行的管理功能有关的安全相关事件，包括改变

TSF 所控制的实体的安全特性；

- g) 管理员指南应当与为评估而提供的其他所有文档保持一致；
- h) 管理员指南应当描述与管理有关的所有 IT 环境的所有安全要求。

4.2.2 用户指南

4.2.2.1 开发者行为元素

开发者应当提供用户指南。

4.2.2.2 证据的内容和形式元素：

- a) 用户指南应该描述网站恢复产品的非管理用户可用的功能和接口；
- b) 用户指南应该描述网站恢复产品提供的用户可访问的安全功能的用法；
- c) 用户指南应该包含受安全处理环境中所控制的用户可访问的功能和权限的警告；
- d) 用户指南应该清晰地阐述网站恢复产品安全运行中用户所必须负的职责，包括有关在网站恢复产品安全环境阐述中找得到的用户行为的假设；
- e) 用户指南应该与为评估而提供的其它所有文档保持一致；
- f) 用户指南应该描述与用户有关的所有 IT 环境的所有安全要求。

5 网站恢复产品安全技术要求的等级划分

依据信息技术网站恢复产品的开发、生产现状及实际应用情况，我们对网站恢复产品的

安全功能要求划分成二个等级。

网站恢复产品安全技术要求等级划分如表 1 所示。

表 1 信息技术网站恢复产品安全等级划分表

		安全功能类	
		基本要求	增强要求
3.1 网页文件自动恢复功能		3.1	3.1
3.2 网页目录自动恢复功能		3.2	3.2
3.3 管理 功能	3.3.1 管理员身份鉴别	3.3.1	3.3.1
	3.3.2 管理员权限	3.3.2	3.3.2
	3.3.3 监控目录/文件管理	3.3.3.1	3.3.3.2
	3.3.4 备份文件的安全存储 及保密传输	3.3.4	3.3.4
	3.3.5 产品自身安全性	3.3.5	3.3.5
	3.3.6 远程管理的安全性		3.3.6
3.4 报警 功能	3.4.1 实时报警	3.4.1	3.4.1
	3.4.2 报警信息的数据格式		3.4.2
	3.4.3 报警方式	3.4.3	3.4.3
3.5 审计日 志功能	3.5.1 可审计事件	3.5.1	3.5.1
	3.5.2 审计信息的数据格式		3.5.2
	3.5.3 审计跟踪管理	3.5.3	3.5.3
	3.5.4 可理解的格式	3.5.4	3.5.4
4 保证要求		4	4
a 基本要求：为网站恢复产品的最底安全级别。			
b 增强要求：为进一步提升产品安全功能的附加要求。			