基本信息

漏洞类型：源码泄露漏洞

漏洞等级：高危

厂商信息：此处需要手动搜索

漏洞简述

漏洞描述

整个网站的源代码文件泄露，包括大量的敏感数据，数据库连接数据 等。

产生原因

1 网站自动备份，备份文件名和路径容易被猜解。  
 2 管理员手动备份文件名，用的域名作为备份文件名称，并且放置在根目录。

漏洞危害

1网站存在备份文件：网站存在备份文件，例如数据库备份文件、网站源码备份文件等，攻击者利用该信息可以更容易得到网站权限，导致网站被黑。  
 2敏感文件泄露是高危漏洞之一，敏感文件包括数据库配置信息，网站后台路径，物理路径泄露等，此漏洞可以帮助攻击者进一步攻击，敞开系统的大门。  
 3 由于目标备份文件打包了多个文件夹，可能存在更多敏感数据泄露  
 4 该备份文件被下载后，可以被用来做代码审计，进而造成更大的危害  
 5 该信息泄露会暴露服务器的敏感信息，使攻击者能够通过泄露的信息进行进一步入侵。

漏洞详情

网站漏洞报表

漏洞地址:http://www.cern.ac.cn/a.zip

文件大小: 42M

网站信息报表

百度权重 1

网站主页 http://www.cern.ac.cn

网站描述 暂无信息

网站标题 中国生态系统研究网络

IP\_\_坐标 北京市 科技网

所属\_\_IP 159.226.111.43

网站年龄 22年3月23天（创建于1997年01月10日,过期时间为2019年07月01日)

备案编号 京ICP备05002858号-6

备案性质 事业单位

备案名称 中国科学院生态环境研究中心

备案时间 2018/11/20 0:00:00

百度收录 暂无信息

协议类型 HTTP/1.1 200 OK

页面类型 text/html

服务类型 Microsoft-IIS/7.0

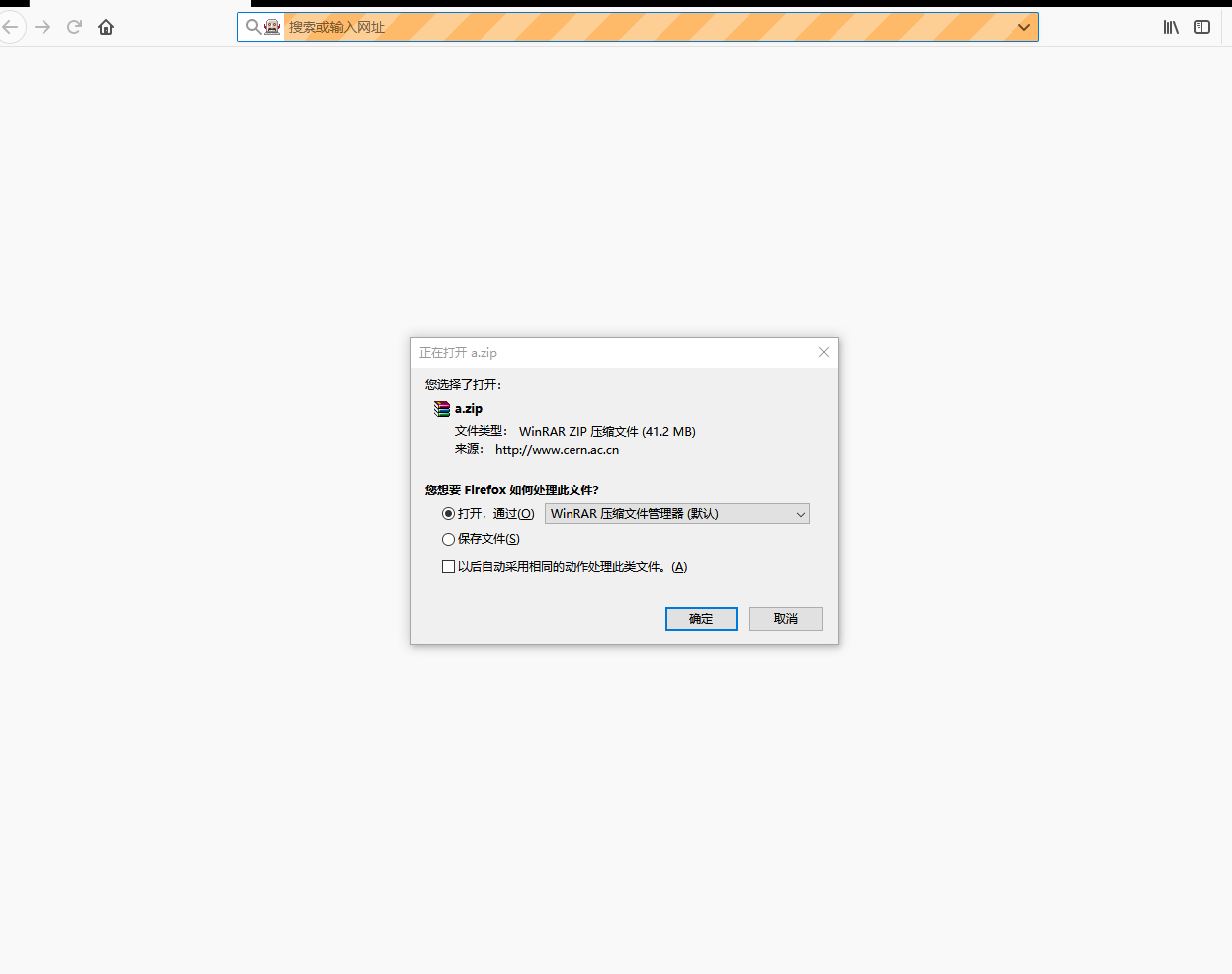
程序语言 暂无信息

网站漏洞复现(使用Firefox浏览器)

下载链接

http://www.cern.ac.cn/a.zip

返回结果



复现完成，验证存在源码泄露漏洞

修复建议

根源上进行修复

1 删除检测出的备份文件，或者将这类文件从网站目录下移走。  
 2 使用非常规的文件名称。  
 3 特定的文件设置合理的权限。  
 4 删除一些不需要的敏感文件。