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

SVN（subversion）是源代码版本管理软件，造成SVN源代码漏洞的主要原因是管理员操作不规范。“在使用SVN管理本地代码过程中，会自动生成一个名为.svn的隐藏文件夹，其中包含重要的源代码信息。但一些网站管理员在发布代码时，不愿意使用‘导出’功能，而是直接复制代码文件夹到WEB服务器上，这就使.svn隐藏文件夹被暴露于外网环境，黑客可以借助其中包含的用于版本信息追踪的‘entries’文件，逐步摸清站点结构。”（可以利用.svn/entries文件，获取到服务器源码、svn服务器账号密码等信息）

漏洞危害

1 SVN产生的.svn目录下还包含了以.svn-base结尾的源代码文件副本（低版本SVN具体路径为text-base目录，高版本SVN为pristine目录），如果服务器没有对此类后缀做解析，黑客则可以直接获得文件源代码。  
 2 可以列出网站目录，甚至下载整站。  
 3 可以直接获取数据库连接信息账号密码，以及后台地址等更多敏感信息。  
 4 可以用来下载该网站源码，做代码审计，发现更大的漏洞造成更大的危害  
 5 网站存在包含SVN信息的文件，这是网站源码的版本控制器私有文件，里面包含SVN服务的地址、提交的私有文件名、SVN用户名等信息，该信息有助于攻击者更全面了解网站的架构，为攻击者入侵网站提供帮助。  
 6 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.4001002003.com/.svn/entries

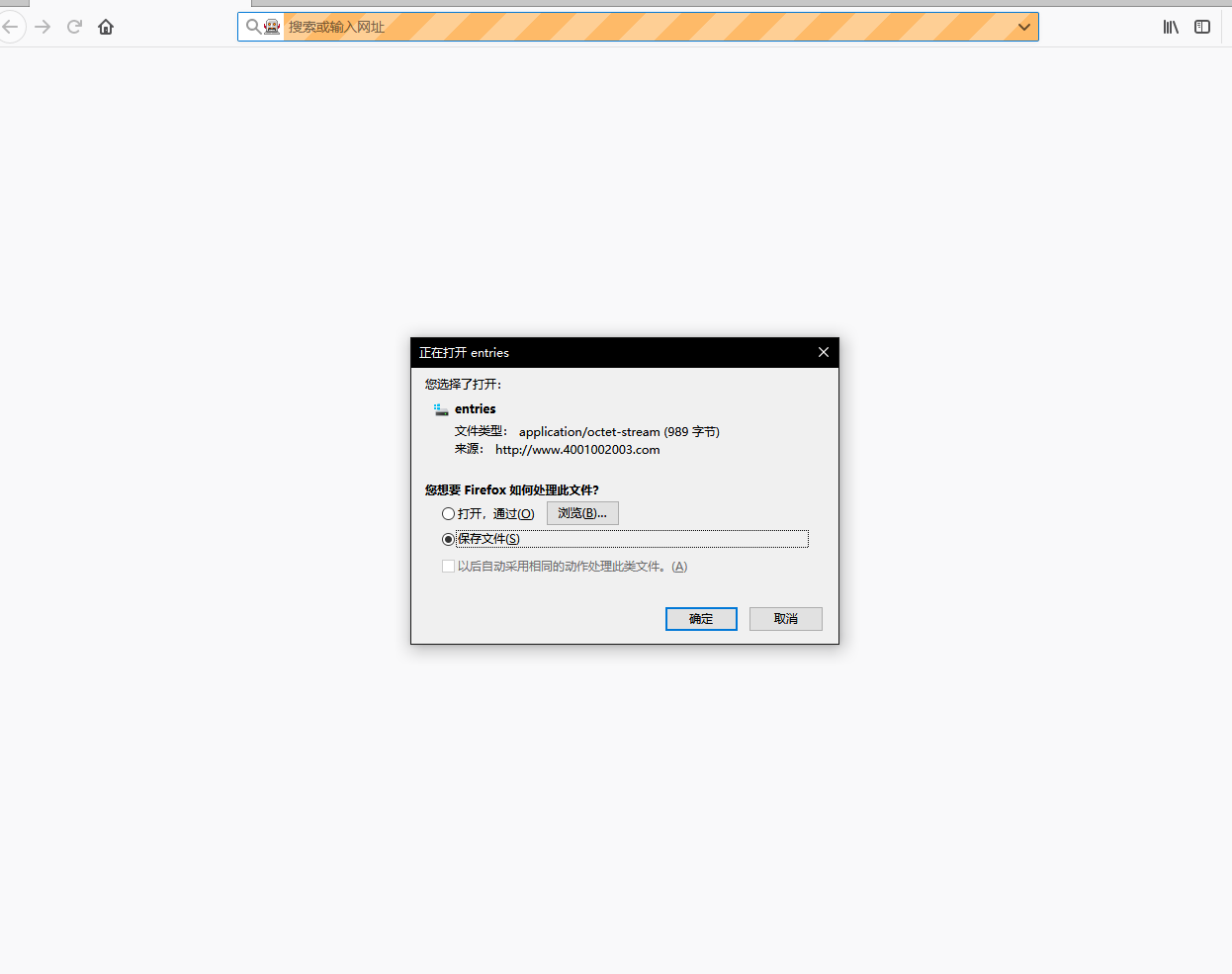
网站信息报表

网站漏洞复现(使用Firefox浏览器)

下载链接

http://www.4001002003.com/.svn/entries

返回结果



源码恢复检测工具

xxxxxx这里手动插图xxxxxxxxxx

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、在web服务器配置文件中增加一段代码，过滤到.svn文件，返回404nginx服务器：  
 location ~ ^(.\*)\/\.svn\/  
 {  
 return 404;  
 }  
 重启nginx  
 Apache服务器：  
 Order allow,deny  
 Deny from all   
 重启Apache  
   
 2、查找服务器上所有.svn隐藏文件夹，删除  
 以下命令删除当前目录下.svn文件夹  
 find . -type d -name ".svn"|xargs rm -rf  
 rm -rf `find . -type d -name .svn`  
 find . -name ".svn" -type d | xargs rm -fr  
 find . -name ".svn" -type d | xargs -n1 rm -R