

# Detailed Threat Analysis Reports: CVE-2023-22527, CVE-2023-46805 and CVE-2024-21887

From the threat prioritization list, I selected three vulnerabilities with the highest CVSS scores. First, I would like to draw attention to CVE-2023-22527 vulnerability in the Atlassian Confluence product. This vulnerability is a template injection vulnerability that causes Remote Code Execution (RCE) attacks and is at a critical level with a CVSS score of 10.0.

The second is CVE-2024-21887 vulnerability in Ivanti Connect Secure and Policy Secure products. This vulnerability contains a command injection vulnerability and is critical with a CVSS score of 9.1. Using CVE-2024-21887 and CVE-2023-46805 together can cause dangerous consequences. For this reason, thirdly, I would like to draw attention to the CVE-2023-46805 vulnerability in Ivanti Connect Secure and Policy Secure products.

## Disclosure of Atlassian Confluence CVE-2023-22527 Vulnerability

Atlassian disclosed CVE-2023-22527, a critical remote code execution (RCE) vulnerability for Confluence Data Center and Confluence Server, on January 16, 2024. This vulnerability is a template injection vulnerability for outdated versions of Confluence Data Center and Server, allowing an unauthenticated attacker to obtain RCE on an affected version.

This vulnerability affects certain versions of Confluence Data Center and Confluence Server. The affected versions are:

- Confluence Data Center and Server 8.0.x, 8.1.x, 8.2.x, 8.3.x, 8.4.x, 8.5.0-8.5.3

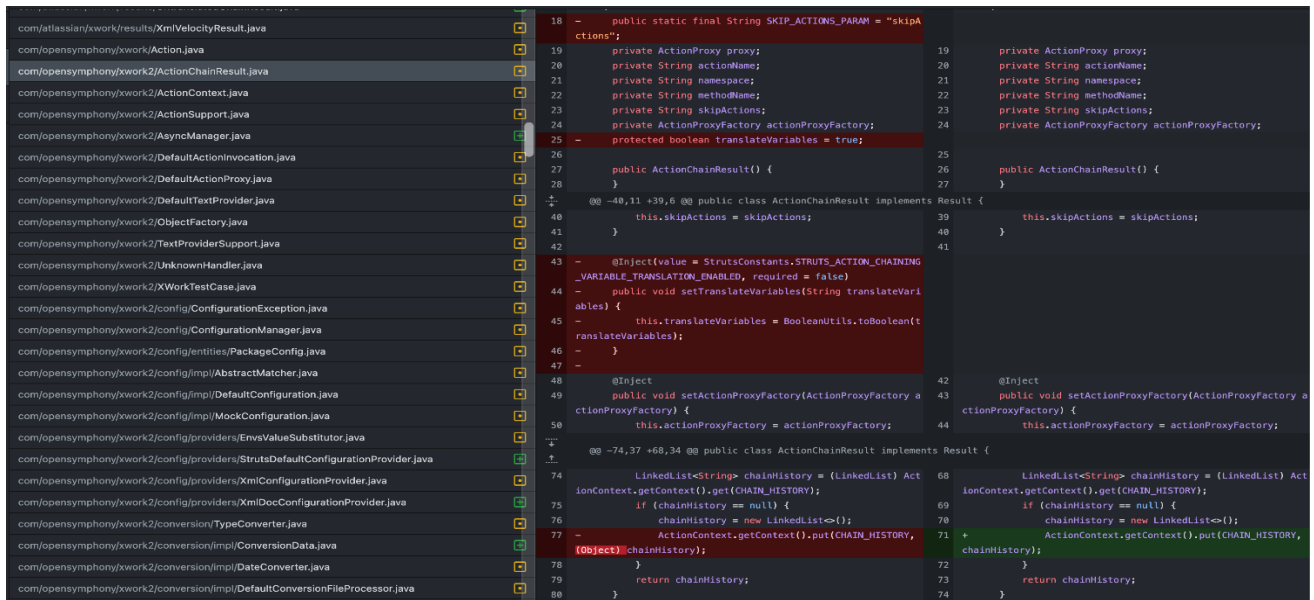
The severity level of this vulnerability is rated critical (9.8) with CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H. A high CVSS score indicates an increase in the seriousness and potential damage of a vulnerability. Therefore, it will attract the attention of threat actors and motivate them to attack the system. Therefore, necessary precautions should be taken urgently.

This vulnerability previously appeared in Atlassian Confluence after two separate OGNL injection vulnerabilities were discovered in September 2021 and June 2022.

## Investigation of Atlassian Confluence CVE-2023-22527 Vulnerability in Technical Details

The ProjectDiscovery team reports that using a technique called "patch diffing", which is often used to understand the effects of a security patch, the team compared the differences between Confluence versions 8.5.4 and 8.5.3 to the patch differences and discovered a significant number of changes between the two versions, including file additions and deletions.

Analyzing the changes, it appears that many files contain OGNL-related changes, often related to code restructuring. However, nothing was found that clearly points to a security vulnerability.



[Screenshot of the patch differences between Confluence v8.5.3 and v8.5.4.](#)

According to Atlassian, this vulnerability was automatically neutralized due to changes made in version 8.5.4. However, with the release of the latest Confluence version 8.5.5, the root cause has been completely eliminated.

## Identification of Unauthenticated Attack Surface in Atlassian Confluence CVE-2023-22527 Vulnerability

To identify this vulnerability as an unauthenticated attack surface, it is important to first understand how Confluence works. Confluence uses Velocity templates for rendering content. These templates can be directly accessed and rendered by the user. But instead of accessing these files only through struts operations, it is said that by accessing **\*.vm** files directly, they can be rendered correctly even if there is an unauthenticated user.

Next, to identify template files that could take potentially harmful parameters and pass them to dangerous OGNL expressions, files that pass parameter values like **\$parameters** directly to dangerous places like **\$ognl.findValue** or **\$stack.findValue** were detected. For example, a template file that accepts the #set parameter is **confluence/template/xhtmll/pagelist.vm**:

```
text-inline.vm  pagelist.vm*  X
/* Don't include this directly! Use ie. general-pagelist.vm instead. */

#set ($pageTitle = $stack.findValue($parameters.pages))
#set ($rawTitle = $!parameters.get('mytitle'))
#if ($rawTitle)
    #set ($labelValue = $!i18n.getText($rawTitle) )
#end
#set ($labelValue = $!rawTitle)
#end

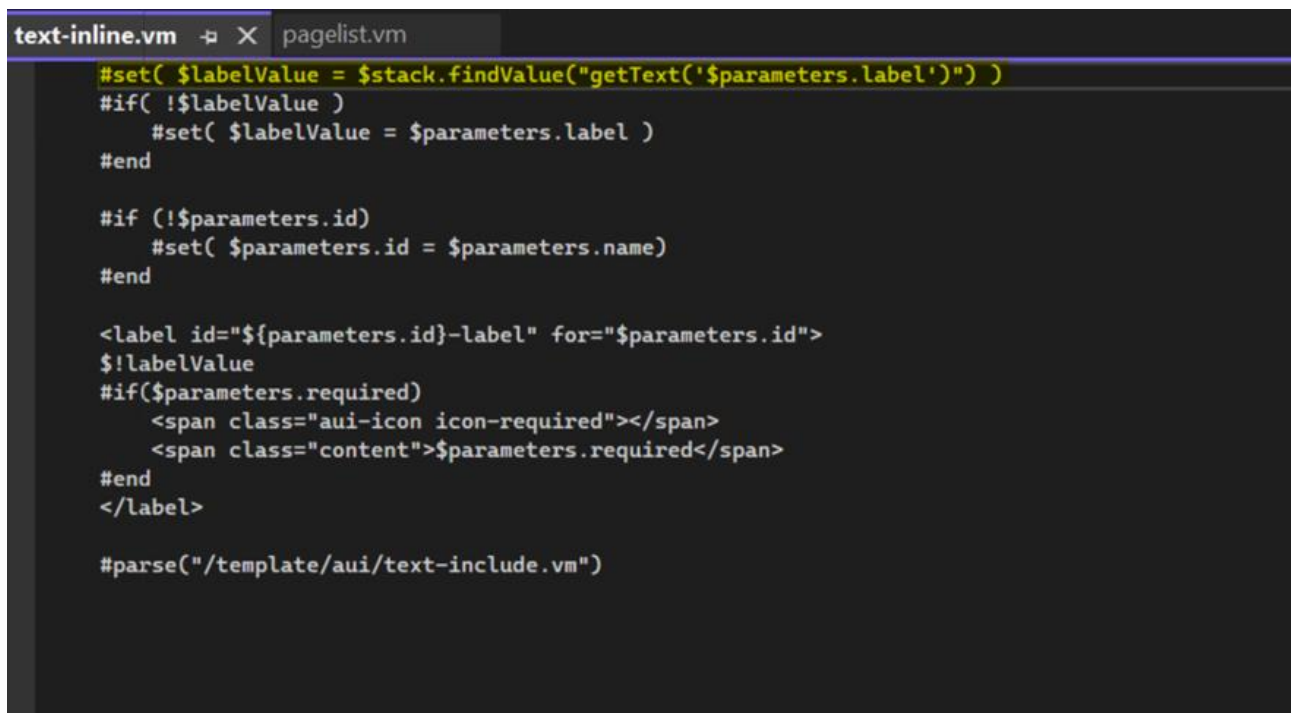
#if ("!$labelValue" != "")
<div class="tabletitle" style="width:$tablewidth">
    #if ($showmore || $showless || $showrss)
        <div style="float:right; valign="bottom" class="tabletitleops">
            &nbsp;
            #if ($showrss)
                <a href="$req.contextPath/spaces/rss.action?key=$htmlUtil.urlEncode($space.key)">img src="$staticResourceUrlPrefix/images/icons/rss.gif" title="RSS"></a>
            &nbsp;
            #end
            #if ($showless)
                <a href="$showless">img src="$staticResourceUrlPrefix/images/icons/subtract_12.gif" title="$textShowLess"></a>
            &nbsp;
            #end
            #if ($showmore)
                <a href="$showmore">img src="$staticResourceUrlPrefix/images/icons/add_12.png" title="$textShowMore"></a>
            &nbsp;
            #end
        </div>
    </div>
    #if ("!$labelValue" != "")
        <h2>$labelValue</h2>
    </div>
#end
```

```
#set ($pageList = $stack.findValue($parameters.pages))
```

Analysts are noticing that `$parameters.pages` can be sent as an object and to fix this situation, it is necessary to add double quotes around `$parameters.pages`. And this change causes OGNL injection.

```
#set ($pageList = $stack.findValue("$parameters.pages"))
```

Then, searching for `findValue` calls in double quotes in `$parameters` found this usage in `confluence/template/au/text-inline.vm`. However, this file was found to have been removed from the current release. In this way, it appears that vulnerability CVE-2023-22527 was detected in the `confluence/template/au/text-inline.vm` endpoint.



```
text-inline.vm  X  pagelist.vm
#set( $labelValue = $stack.findValue('getText('$parameters.label')') )
#if( !$labelValue )
    #set( $labelValue = $parameters.label )
#end

#if ( !$parameters.id )
    #set( $parameters.id = $parameters.name )
#end

<label id="{parameters.id}-label" for="{parameters.id}">
    $!labelValue
    #if($parameters.required)
        <span class="au-icon icon-required"></span>
        <span class="content">$parameters.required</span>
    #end
</label>

#parse("/template/au/text-include.vm")
```

```
#set( $labelValue = $stack.findValue("getText('$parameters.label')") )
```

The source of this vulnerability was found to be the `&stack.findValue` function, and the fact that the value from the tag parameter was passed directly to this function identified the presence of a template injection vulnerability. As a result, it was found that a remote code execution vulnerability could be created by exiting the call to the `_getText` function and injecting malicious OGNL.

## CVE-2023-22527 Size of Attack Surface

We can quickly find a large number of Confluence servers using some intelligence platforms to gather some data about public Confluence servers.

- The [Shodan](#) platform found close to 63,000 Confluence servers with the `http.component` query: "Atlassian Confluence"



- [ZoomEye](#) found more than 600,000 results with the query **app: "Atlassian Confluence"** and 70,000 Confluence servers with the query **app: "Atlassian Confluence" +title: "Log In - Confluence"** by making the query a bit more specific.

app:"Atlassian Confluence" +title:"Log In - Confluence"

About 70,179 results (Nearly year: 61,462 results) 5.973 seconds

app:"Atlassian Confluence" × +title:"Log In - Confluence" ×

IP	Location	ASN	Banner	File
16.170.101.101	Sweden, Stockholm	AS16509	7180/http/TCP	HTTP/1.0 200 OK Date: Sun, 18 Feb 2024 00:52:27 GMT Server: nginx Content-Length: 31645 Content-Type: text/html

SEARCH TYPE

Search Type	Count
Devices	69,571
Ipv4	69,491
Ipv6	80
Websites	506

- [HunterHow](#) found close to 66,000 Confluence servers with the query **product.name="Confluence"**.

product.name="Confluence"

Results 220,600 Filter: Past month

IP	Location	ASN	Web Title	Protocol	Trans Protocol	Header	App/Product
47.95.104.80	Beijing, China	80	Log In - Confluence	http	tcp	HTTP/1.1 200 OK X-Xss-Protection: 1; mode=block Content-Type: text/html; charset=UTF-8 Connection: keep-alive Content-Security-Policy: frame-ancestors 'self' Date: Sat, 17 Feb 2024 20:25:02 GMT Expires: Thu, 01 Jan 1970 00:00:00 GMT	200 2024-02-18 GMT +8
40.103.104.109	Zagreb, Croatia	1027	Log In - Atlassian - Confluence	https	tcp	HTTP/1.1 200 OK Content-Security-Policy: frame-ancestors 'self' Content-Type: text/html; charset=UTF-8 Strict-Transport-Security: max-age=15768000 X-Confluence-Request-Time: 1697033191190 X-Content-Type-Options: nosniff X-Frame-Options: SAMEORIGIN	200 2024-02-18 GMT +8

**Statistics**

Category	Count
Total IP Count	65.6K
Internet Services	220.6K

**Filter Mode**

**By Location**

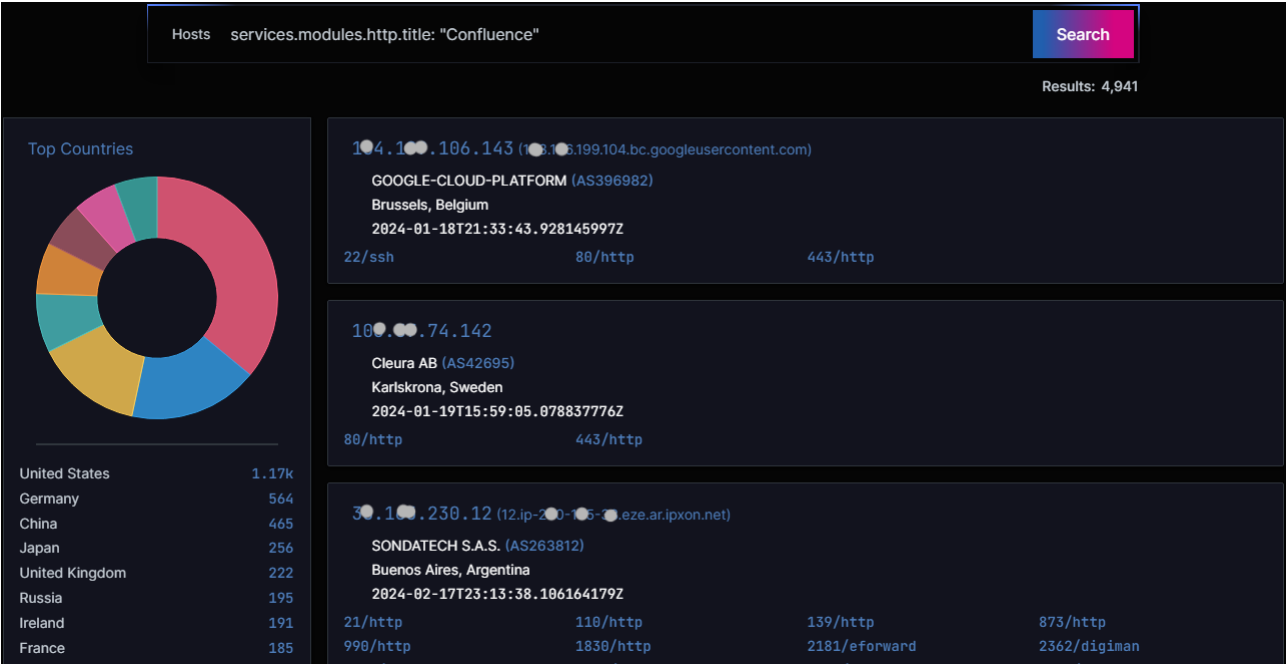
Location	Count
China	70K
South Africa	32.6K
United States	30.3K
Japan	11K
Germany	7.5K

**By Port**

Port	Count
443	14K

But the reality of these searches is that these internet search platforms show a much higher number of results than they actually are. We also know that these results include honeypots. According to a study done by [VulnCheck](#) using shodan, there are approximately 236,000 Confluence honeypots on the internet and the actual number of Confluence servers is around 4200.

Additionally, in the [ODIN platform](#), a quick search using the term **"services.modules.http.title: Confluence"** reveals that there are over 4,000 Confluence instances exposed on the internet. These instances are primarily located in the United States, Germany, China, Russia, Japan, and the United Kingdom, which significantly increases the potential attack surface.



# Detailed Threat Analysis Reports: CVE-2023-46805 and CVE-2024-21887:

## Disclosure of CVE-2023-46805 and CVE-2024-21887 Vulnerabilities

On January 10, 2024, Ivanti issued a security advisory about two zero-day vulnerabilities affecting Ivanti Connect Secure and Policy Secure. Vulnerability CVE-2023-46805 is an authentication bypass vulnerability with a CVSS score of 8.2 (High) and vulnerability CVE-2024-21887 is an instruction injection vulnerability with a CVSS score of 9.1 (Critical). Attackers were observed using the vulnerabilities together to remotely execute code on vulnerable Ivanti products.

This vulnerability affects certain versions of Ivanti Connect Secure and Policy Secure. The affected versions are:

- Ivanti Connect Secure versions 9.x and 22.x
- Ivanti Policy Secure versions 9.x and 22.x

CVE-2024-21887 vulnerability is rated critical (9.1) with the following vector CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H and CVE-2023-46805 vulnerability is rated high (8.2) with the following vector CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:N. A high CVSS score indicates an increase in the severity and potential damage of a vulnerability. Therefore,

it will attract the attention of threat actors and motivate them to attack the system. Therefore, necessary precautions should be taken urgently.

## Technical Analysis of CVE-2023-46805 and CVE-2024-21887 Vulnerabilities

An examination of CVE-2023-46805 (Authentication Bypass) and CVE-2024-21887 (Remote Command Execution), two critical vulnerabilities recently disclosed by Ivanti that affect Ivanti Pulse Connect Secure products, reveals a complex security risk. This report will discuss the technical details and potential impact of both vulnerabilities in detail.

### CVE-2023-46805: Authentication Bypass Vulnerability

CVE-2023-46805 is an authentication bypass vulnerability in Ivanti Pulse Connect Secure VPN products. This vulnerability targets the `"/api/v1/totp/user-backup-code"` endpoint. Using this endpoint, attackers can bypass the authentication mechanism and gain unauthorized access. This can lead to the system being vulnerable to unauthorized access and sensitive data being accessed.

Technically, this vulnerability is caused by the inadequacy of authentication on the targeted endpoint. Attackers target an endpoint that does not require authentication and thus gain unauthorized access. This allows attackers to log into the system and perform unauthorized operations.

#### To test a vulnerability called CVE-2023-46805:

```
//Example GET Request to test for CVE-2023-46805
```

```
GET /api/v1/totp/user-backup-code/../../../../system/system-information
```

```
HTTP/1.1 Host: <IP_Vulnerable_Ivanti_Product>
```

```
Content-Length: 0
```

```
//Response from the vulnerable product
```

```
...
```

```
"system-information" : {
```

```
  "Cluster-node" : { },
```

```
  "Hardware-model" : "PSA-3000",
```

```
  "host-name" : <redacted>
```

```
  "machine-id" : <redacted>
```

```
  "os-name" : "ive-sa",
```

```
  "os-version" : "9.1R18.1",
```

```
  "serial-number": <redacted>
```

```
}
```

```
...
```

```
POST /api/v1/totp/user-backup-code/../../../../system/platform?operation=testConnectivity
```

## Attack Vector and Exploitation

This vulnerability is due to a weakness in an authentication mechanism in the web interface. By bypassing a specific authentication step in the web interface or using spoofing methods, attackers can access areas that they are not normally authorized to access. This allows attackers to log into the system without authorization and access sensitive data.

## Impacts

CVE-2023-46805 vulnerability, when successfully exploited, can result in unauthorized access to devices. This allows attackers to access gateways and gain access to the organization's sensitive data. Furthermore, by exploiting this vulnerability, organizations could risk significant data loss and reputational damage.

## CVE-2024-21887: Remote Command Execution Vulnerability

CVE-2024-21887 is a remote command execution vulnerability in Ivanti Pulse Connect Secure products. This vulnerability exists in the API endpoint `"/api/v1/license/keys-status/path:node_name"`. Using this endpoint, attackers can perform command injection and execute unwanted commands to the target system. This has the potential to compromise the system and perform unauthorized operations.

Technical analysis of this vulnerability shows that it is caused by inadequate auditing of user input on the targeted endpoint. Attackers can combine user-supplied data with malicious commands, which become executable on the target system. This allows the system to be exploited and attackers to perform unauthorized operations.

```
GET /api/v1/totp/user-backup-code/../../license/keys-status/<url_encoded_python_reverse_shell>  
HTTP/1.1 Host: <IP_Vulnerable_Ivanti_Product>
```

This code represents an attempt to exploit known vulnerabilities in Ivanti Pulse Connect Secure to gain unauthorized remote access to the server.

## Attack Vector and Exploitation

This vulnerability is due to a weakness in the processing of specially crafted requests sent to devices. By sending specially crafted requests to exploit this vulnerability, attackers can cause arbitrary commands to execute on devices. This allows attackers to execute arbitrary commands on devices and make arbitrary changes to systems.

## Impacts

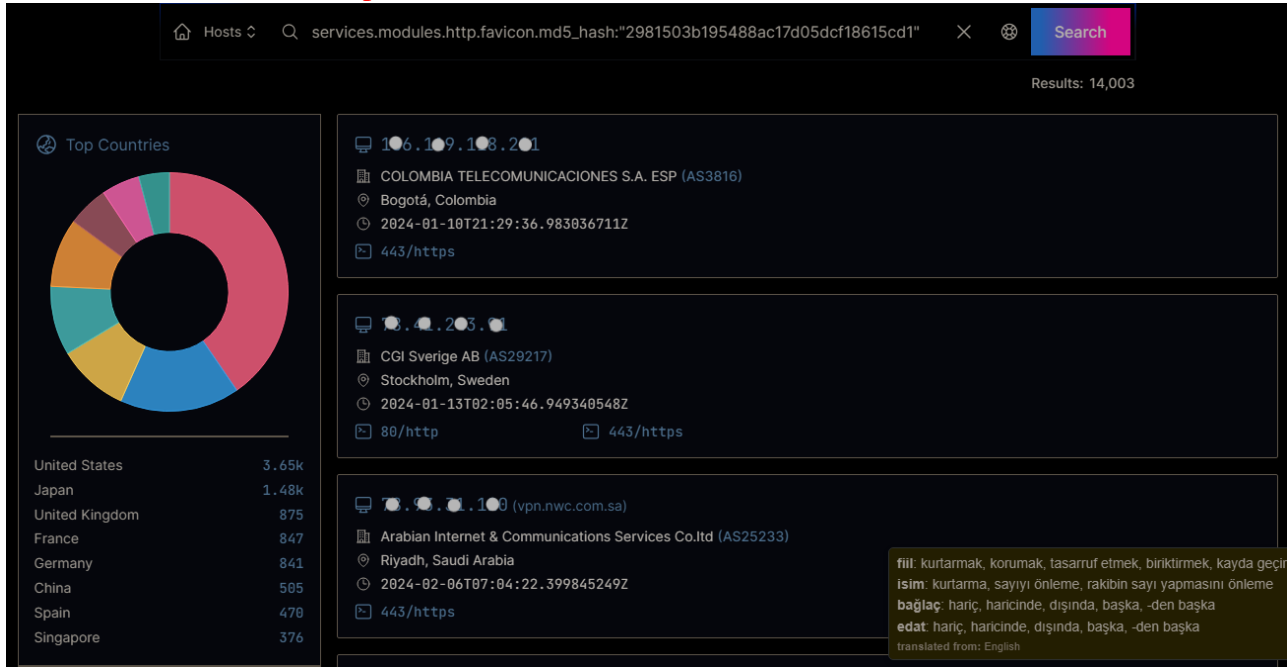
CVE-2024-21887 vulnerability, when successfully exploited, can cause arbitrary commands to execute on devices. This allows attackers to execute arbitrary commands on devices and make arbitrary changes to systems. Furthermore, by exploiting this vulnerability, organizations could risk significant data loss and reputational damage.



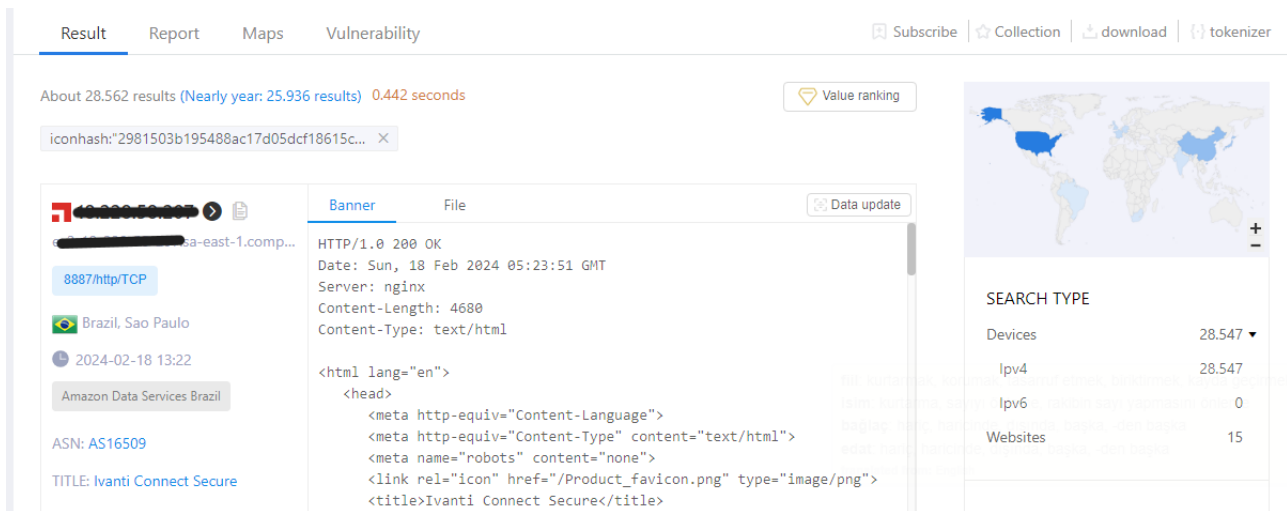
# Size of the Attack Surface in CVE-2023-46805 and CVE-2024-21887 Vulnerabilities

We can quickly find a large number of Ivanti VPN servers by using some intelligence platforms to collect some data from publicly available sources.

- The [ODIN platform](#) found close to 14,000 Ivanti VPN servers by querying `services.modules.http.favicon.md5_hash: "2981503b195488ac17d05dcf18615cd1"`.



- The [ZoomEye platform](#) found close to 29,000 Ivanti VPN servers with the query `iconhash: "2981503b195488ac17d05dcf18615cd1"`.





- The [Shodan platform](#) found 43,000 Ivanti VPN servers by querying <http://favicon.hash:1439222863>.



The non-profit risk monitoring service [Shadowserver](#) is currently monitoring more than 16,800 ICS VPN home equipment detected online, almost 5,000 of which are US-based servers.

## REFERENCES

1. SecureStack. (2023, September 27). Confluence-Aggedon! Atlassian Confluence Vulnerabilities CVE-2023-22515 and CVE-2023-22518. <https://confluence.atlassian.com/display/CONF719/Best+Practices+for+Configuring+Confluence+Security>
2. Cyble. (2023, September 28). Active Exploitation of Atlassian Confluence RCE Vulnerability (CVE-2023-22527). [<https://cyble.com/blog/exploitation-of-atlassian-confluence-rce-vulnerability-cve-2023-22527/>]
3. Arctic Wolf. (2023, September 29). Exploitation of Confluence Server Vulnerability CVE-2023-22527 Leading to C3RB3R Ransomware. [<https://arcticwolf.com/resources/blog/confluence-cve-2023-22527-leading-to-c3rb3r-ransomware/>]
4. Project Discovery. (2023, September 27). Atlassian Confluence - Remote Code Execution (CVE-2023-22527). [<https://confluence.atlassian.com/display/KB/FAQ+for+CVE-2023-22527>]
5. VulnCheck. (2023, October 26). There Are Too Many Damn Honeypots. [<https://vulncheck.com/blog/too-many-honeypots>]
6. Atos. (2024, January 23). Analysis of Ivanti 0-days, CVE-2023-46805 and CVE-2024-21887. [<https://atos.net/en/lp/securitydive/analysis-of-ivanti-0-days-cve-2023-46805-and-cve-2024-21887>]
7. Volexity. (2024, January 10). Active Exploitation of Two Zero-Day Vulnerabilities in Ivanti Connect Secure VPN. [<https://www.volexity.com/blog/2024/01/10/active-exploitation-of-two-zero-day-vulnerabilities-in-ivanti-connect-secure-vpn/>]
8. Assetnote. (2023, December 19). High Signal Detection and Exploitation of Ivanti's Pulse Connect Secure Auth Bypass & RCE. [<https://www.assetnote.io/resources/research/high-signal-detection-and-exploitation-of-ivantis-pulse-connect-secure-auth-bypass-rce>]
9. Mandiant. (2023, December 22). Cutting Edge: Suspected APT Targets Ivanti Connect Secure VPN in New Zero-Day Exploitation. [<https://www.mandiant.com/resources/blog/suspected-apt-targets-ivanti-zero-day>]
10. Dormann, W. ([n.d.]). Will Dormann (@wdormann@infosec.exchange). [<https://infosec.exchange/@wdormann/111773557274385196>]
11. Rapid7. (2023, August 21). CVE-2023-46805. [<https://attackerkb.com/topics/AdUh6by52K/cve-2023-46805/rapid7-analysis>]