

Wipro Holmes Orchestrator 20.4.1 Report Disclosure

Authored by [Rizal Muhammed](#)

Posted Nov 22, 2021

Wipro Holmes Orchestrator version 20.4.1 allows unauthenticated re-downloading of priory exported reports in Excel.

tags | [exploit](#) | [info disclosure](#) | [advisories](#) | [CVE-2021-38147](#)

SHA-256 | [be9d06f0cfd4b2a5e3e1048b978ac6ba226c9ce6a52b1ce78d912d5e71b418e](#) [Download](#) | [Favorite](#) | [View](#)

Related Files

Share This

Like Tweet LinkedIn Reddit Digg StumbleUpon

Change Mirror

Download

```
# Exploit Title: Wipro Holmes Orchestrator 20.4.1 Unauthenticated Excel Report Download
# Date: 09/08/2021
# Exploit Author: Rizal Muhammed @ub3rs1ck
# Vendor Homepage: https://www.wipro.com/holmes/
# Version: 20.4.1
# Tested on: Windows 10 x64
# CVE : CVE-2021-38147

In the Wipro Holmes Orchestrator 20.4.1 application, if at some point some user has exported any of the Reports as excel, these files remain in the server. When an unauthenticated user attempts to access any of the below endpoints such files are downloaded. Details of the vulnerable endpoints and the information exposed by the reports from these endpoints are provided below.

User Report:-
API: http://HOLMES_ORCH_HOST:PORT/processexecution/DownloadExcelFile/User_Report_Excel
Exposed Information: Username, Email, Role, First Name, Last Name, User Level and User Domain of different users.

Domain Credentials Report:-
API: http://HOLMES_ORCH_HOST:PORT/processexecution/DownloadExcelFile/Domain_Credential_Report_Excel
Exposed Information: Domain Credential Names, Type, Domain Names

Other Endpoints:-
http://HOLMES_ORCH_HOST:PORT/processexecution/DownloadExcelFile/Process_Report_Excel
http://HOLMES_ORCH_HOST:PORT/processexecution/DownloadExcelFile/Infrastructure_Report_Excel
http://HOLMES_ORCH_HOST:PORT/processexecution/DownloadExcelFile/Resolver_Report_Excel
```

[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
nu11securlty 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)	December 2022
Advisory (79,754)	November 2022
Arbitrary (15,694)	October 2022
BBS (2,859)	September 2022
Bypass (1,619)	August 2022
CGI (1,018)	July 2022
Code Execution (6,926)	June 2022
Conference (673)	May 2022
Cracker (840)	April 2022
CSRF (3,290)	March 2022
DoS (22,602)	February 2022
Encryption (2,349)	January 2022
Exploit (50,359)	Older
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



© 2022 Packet Storm. All rights reserved.

Site Links

- News by Month

News Tags

Files by Month

File Tags

File Directory

About Us

- History & Purpose

Contact Information

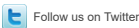
Terms of Service

Privacy Statement

Copyright Information

Hosting By

Rokasec



Follow us on Twitter



Subscribe to an RSS Feed