MonoCMS Blog 1.0 File Deletion / CSRF / Hardcoded Credentials

Authored by Shahrukh Iqbal Mirza | Posted Oct 1, 2020

MonoCMS Blog version 1.0 suffers from arbitrary file deletion, cross site request forgery, and information disclosure vulnerabilities.

tags | exploit, arbitrary, vulnerability, file inclusion, info disclosure, csrf
advisories | CVE-2020-25986, CVE-2020-25987
SHA-256 | 94d8b82b640c31f62e5544ec3f22c4fb6cfbe03963f5dca9e93d0c74da17b5cf | Download | Favorite | View

Related Files

Share This

Like Twee LinkedIn Reddit Digg StumbleUpon

Change Mirror | Download

```
# Exploit Title: MonoCMS Blog 1.0 - Arbitrary File Deletion (Authenticated)
# Date: 2020-09-20
# Exploit Author: Shahrukh Iqbal Mirza (@shahrukhiqbal24)
# Vendor Homepage: https://monocms.com/download
# Software Link: https://monocms.com/download
# Version: 1.0
# Tested On: Windows 10 (XAMPP)
# CVE: N/A

Proof of Concept:
1.  In the upload images page, make a request to delete an already uploaded image. If no image present, upload
an image and then make a request to delete that image.
2.  Notice the Request URL
<ip>/base_path_to_cms/uploads?delimg=../../../../../Temp/Copy.txt
This deletes the file 'copy.txt' from C:\Temp
3.  Use simple directory traversals to delete arbitrary files.

Note: php files can be unlinked and not deleted.


------------------------------------------------------------------------------------------------------------------------
########################################################################################################################
------------------------------------------------------------------------------------------------------------------------

# Exploit Title: MonoCMS Blog - Account Takeover (CSRF)
# Date: September 29th, 2020
# Exploit Author: Shahrukh Iqbal Mirza (@shahrukhiqbal24)
# Vendor Homepage: https://monocms.com/download
# Software Link: https://monocms.com/download
# Version: 1.0
# Tested On: Windows 10 (XAMPP)
# CVE: CVE-2020-25986


Proof of Concept:
Login using a test user (attacker). Make a password change request, and enter a new password and then intercept
the request (in BurpSuite). Generate a CSRF PoC. Save the HTML code in an html file. Login as another user
(victim), open the CSRF-PoC html file, and click on submit request. Victim user's password will be changed.


------------------------------------------------------------------------------------------------------------------------
########################################################################################################################
------------------------------------------------------------------------------------------------------------------------

# Exploit Title: MonoCMS Blog - Sensitive Information Disclosure (Hardcoded Credentials)
# Date: September 29th, 2020
# Exploit Author: Shahrukh Iqbal Mirza (@shahrukhiqbal24)
# Vendor Homepage: https://monocms.com/download
# Software Link: https://monocms.com/download
# Version: 1.0
# Tested On: Windows 10 (XAMPP)
# CVE: CVE-2020-25987


Proof of Concept:
Hard-coded admin and user hashes can be found in the "log.xml" file in the source-code files for MonoCMS Blog.
Hash type is bcrypt and hashcat mode 3200 can be used to crack the hash.
```

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 150 files
- Ubuntu 68 files
- LiquidWorm 23 files
- Debian 16 files
- malvuln 11 files
- nu11secur1ty 11 files
- Gentoo 9 files
- Google Security Research 6 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