Joomla! 4.1.0 Zip Slip File Overwrite / Path Traversal

Authored by EgiX | Site karmainsecurity.com

Posted Mar 30, 2022

Joomla! versions 4.1.0 and below suffer from path traversal and file overwrite vulnerabilities due to misplaced trust in the handling of compressed archives.

tags | exploit, vulnerability
advisories | CVE-2022-23793
SHA-256 | 3659bb2a193b54ec58750cfb109d9f00cfd739f7828d6a6d4fdff0e0ff2be911

Download | Favorite | View

Related Files

Share This

Like 0 Tweet LinkedIn Reddit Digg StumbleUpon

Change Mirror Download

```
-------------------------------------------------
Joomla! <= 4.1.0 (Tar.php) Zip Slip Vulnerability
-------------------------------------------------


[-] Software Link:

http://www.joomla.org/


[-] Affected Versions:

Version 4.1.0 and prior versions.
Version 3.10.6 and prior versions.


[-] Vulnerability Description:

The vulnerability is located in the
/libraries/vendor/joomla/archive/src/Tar.php script. Specifically, into
the Joomla\Archive\Tar::extract() method:

113.      $this->getTarInfo($this->data);
114.
115.      for ($i = 0, $n = \count($this->metadata); $i < $n; $i++)
116.      {
117.        $type = strtolower($this->metadata[$i]['type']);
118.
119.        if ($type == 'file' || $type == 'unix file')
120.        {
121.          $buffer = $this->metadata[$i]['data'];
122.          $path   = Path::clean($destination . '/' .
$this->metadata[$i]['name']);
123.
124.          // Make sure the destination folder exists
125.          if (!Folder::create(\dirname($path)))
126.          {
127.            throw new \RuntimeException('Unable to create destination
folder ' . \dirname($path));
128.          }
129.
130.          if (!File::write($path, $buffer))
131.          {
132.            throw new \RuntimeException('Unable to write entry to file ' .
$path);
133.          }
134.        }
135.      }

The vulnerability exists because the above code is using the filename
within the Tar archive ($path variable created at line 122) to write the
extracted file by using File::write() at line 130, without properly
verifying the destination path. This could be exploited to carry out Zip
Slip (or Path Traversal) attacks and write/overwrite arbitrary files,
potentially resulting in execution of arbitrary PHP code or other
dangerous impacts. In the Joomla! core, successful exploitation of this
vulnerability would require administrator privileges. However, there
could be third-party components using the
Joomla\Archive\Archive::extract() method. In such cases, this might
potentially be exploited also by unauthenticated attackers, depending on
the context.


[-] Solution:

Upgrade to version 3.10.7, 4.1.1, or later.


[-] Disclosure Timeline:

[19/02/2021] - Vendor notified
[21/02/2021] - Vulnerability acknowledged by the vendor
```

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
nu11secur1ty 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)

```
[21/02/2021] - Vendor sent details about a proposed patch
[21/02/2021] - Sent feedback about the patch correctness
[29/03/2022] - Vendor update released
[29/03/2022] - Public disclosure


[-] CVE Reference:

The Common Vulnerabilities and Exposures project (cve.mitre.org)
has assigned the name CVE-2022-23793 to this vulnerability.


[-] Credits:

Vulnerability discovered by Egidio Romano.


[-] Other References:

https://developer.joomla.org/security-centre/870-20220301


[-] Original Advisory:

http://karmainsecurity.com/KIS-2022-05
```

Login or Register to add favorites

Intrusion Detection (866)
Java (2,888)
JavaScript (817)
Kernel (6,255)
Local (14,173)
Magazine (586)
Overflow (12,390)
Perl (1,417)
PHP (5,087)
Proof of Concept (2,290)
Protocol (3,426)
Python (1,449)
Remote (30,009)
Root (3,496)
Ruby (594)
Scanner (1,631)
Security Tool (7,768)
Shell (3,098)
Shellcode (1,204)
Sniffer (885)
Spoof (2,165)
SQL Injection (16,089)
TCP (2,377)
Trojan (685)
UDP (875)
Virus (661)
Vulnerability (31,104)
Web (9,329)
Whitepaper (3,728)
x86 (946)
XSS (17,478)
Other

BSD (370)
CentOS (55)
Cisco (1,917)
Debian (6,620)
Fedora (1,690)
FreeBSD (1,242)
Gentoo (4,272)
HPUX (878)
iOS (330)
iPhone (108)
IRIX (220)
Juniper (67)
Linux (44,118)
Mac OS X (684)
Mandriva (3,105)
NetBSD (255)
OpenBSD (479)
RedHat (12,339)
Slackware (941)
Solaris (1,607)
SUSE (1,444)
Ubuntu (8,147)
UNIX (9,150)
UnixWare (185)
Windows (6,504)
Other