

Search		
Soorob		
Search		

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

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

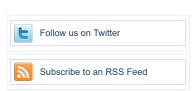
advisories | CVE-2022-23793

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);
115.
116.
117.
                for ($i = 0, $n = \count($this->metadata); $i < $n; $i++)
                   $type = strtolower($this->metadata[$i]['type']);
118.
119.
                   if ($type == 'file' || $type == 'unix file')
 120.
121.
122.
                      $buffer = $this->metadata[$i]['data'];
$path = Path::clean($destination . '/'
123.
                       // Make sure the destination folder exists
125.
                      if (!Folder::create(\dirname($path)))
                      { throw new \mbox{\sc RuntimeException('Unable to create destination })}
 folder ' . \dirname($path));
 129.
130.
                      if (!File::write($path, $buffer))
131.
                         throw new \RuntimeException('Unable to write entry to file ' .
 $path);
 133.
134.
The vulnerability exists because the above code is using the filename within the Tar archive ($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
[-] 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
```



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 186 files
Jbuntu 52 files
Gentoo 44 files
Oebian 27 files
Apple 25 files
Google Security Research 14 files
nalvuln 10 files
u11secur1ty 6 files
njurczyk 4 files
George Tsimpidas 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 June 2022 May 2022 April 2022 March 2022			
CGI (1,015)				
Code Execution (6,913)				
Conference (672)				
Cracker (840)				
CSRF (3,288)	February 2022 January 2022 December 2021			
DoS (22,541)				
Encryption (2,349)				
	Older			
Exploit (50,293)				
File Inclusion (4,162)	Systems			
File Upload (946)				
Firewall (821)	AIX (426)			

Info Disclosure (2,656)

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) 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) 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) UDP (875) Windows (6,504) Virus (661) Other

Vulnerability (31,104)

Web (9,329)

Whitepaper (3,728)

x86 (946) XSS (17,478) Other



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

History & Purpose Contact Information Terms of Service Privacy Statement Copyright Information

About Us

Hosting By

Rokasec



Follow us on Twitter

