

	harver 201111										Search	Search		
what you don't know can hurt you														
T	Home	1	Files		News	I	About	1	Contact	&[SERVICES_TAB]	Add New	I		

ExpressionEngine 6.0.2 PHP Code Injection

Authored by EgiX | Site karmain

Posted Mar 15, 2021

ExpressionEngine versions 6.0.2 and below suffer from a Translate::save PHP code injection vulnerability.

tags | exploit, php advisories | CVE-2021-27230

Related Files

Share This

Lik€

LinkedIn

Reddit

Digg StumbleUpon

Change Mirror Download ExpressionEngine <= 6.0.2 (Translate::save) PHP Code Injection Vulnerability [-] Software Link: https://expressionengine.com/ [-] Affected Versions: Version 6.0.2 and prior versions. Version 5.4.1 and prior versions. [-] Vulnerability Description: The vulnerable code is located in the "ExpressionEngine\Controller\Utilities\Translate::save()" method: private function save(\$language, \$file) \$file = ee()->security->sanitize_filename(\$file); \$dest_dir = \$this->languages_dir . \$language . '/'; \$filename = \$file . '_lang.php'; \$dest_loc = \$dest_dir . \$filename; $str = '<?php' . "\n" . 'slang = array(' . "\n\n'n";$ ee()->lang->loadfile(\$file); 377. 378. "\'"), \$val); 379. 380. .'\'' . ",\n\n"; \$str .= '\'' . \$key . '\' => ' . "\n" . '\'' . \$val 381. 382. 383. 384. \$str .= "''=>''\n);\n\n";
\$str .= "// End of File"; 400. 401. 402. 403. 404. 405. 406. \$dest_loc)) 407. \$this->load->helper('file'); if (write_file(\$dest_loc, \$str)) {
 ee('CP/Alert') -> makeInline('shared-form')
 -> asSuccess()
 -> withTitle(lang('translations_saved'))
 -> addToBody(sprintf(lang('file_saved'), User input passed via keys of POST parameters is not properly sanitized before being assigned to the "9st" variable at line 380. Such a variable will be used in a call to the "str" variable at line 380. Such a variable will be used in a call to the "write_file()" function at line 402, trying to write user supplied content into the /system/user/language/[lang]/[file] lang.php file. This can be exploited to lighting described and execute arbitrary PMP code. Successful exploitation of permissions to access the CP translation system utilities. Upgrade to version 6.0.3, 5.4.2, or later. [-] Disclosure Timeline: .03/02/2021] - Vendor notified through Hackerone [15/02/2021] - Vulnershiltry acknowledged by the vendor [16/02/2021] - CVE number assigned [17/02/2021] - Version 6.0.3 released [04/03/2021] - Version 5.4.2 released [18/03/2021] - Public disclosure [-] CVE Reference: The Common Vulnerabilities and Exposures project (cve.mitre.org) has assigned the name CVB-2021-27230 to this vulnerability. Vulnerability discovered by Egidio Romano. [-] Other References: https://hackerone.com/reports/1093444 [-] Original Advisory: http://karmainsecurity.com/KIS-2021-03

Login or Register to add favorites

E	Follow us on Twitter
<u>y</u>	Subscribe to an RSS Feed

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								
•	Autho		Last	30 D	ays			
Ubuntu 76 files								
LiquidWorm 23 files								
Debian 21 files								
nu11secur1ty 11 files								
malvuln 11 files								
Gentoo 9 files								
Google Security Research 8 files								

Julien Ahrens 4 files

File Archives

T. Weber 4 files

File Tags

rage	
ActiveX (932)	December 2022
Advisory (79,754)	November 2022
Arbitrary (15,694)	October 2022
BBS (2,859)	September 2022
Bypass (1,619)	August 2022
CGI (1,018)	July 2022
Code Execution (6,926)	June 2022
Conference (673)	May 2022
Cracker (840)	April 2022
CSRF (3,290)	March 2022
DoS (22,602)	February 2022
Encryption (2,349)	January 2022
Exploit (50,359)	Older
File Inclusion (4,165)	
File Upload (946)	Systems
Firewall (821)	AIX (426)
Info Disclosure (2,660)	Apple (1,926)
Intrusion Detection (867)	BSD (370)
Java (2,899)	CentOS (55)
JavaScript (821)	Cisco (1,917)
Kernel (6,291)	Debian (6,634)
Local (14,201)	Fedora (1,690)
Magazine (586)	FreeBSD (1,242)
Overflow (12,419)	Gentoo (4,272)
Perl (1,418)	HPUX (878)
PHP (5,093)	iOS (330)
Proof of Concept (2,291)	iPhone (108)
Protocol (3,435)	IRIX (220)
Python (1,467)	Juniper (67)
Remote (30,044)	Linux (44,315)
Root (3,504)	Mac OS X (684)
Ruby (594)	Mandriva (3,105)
Scanner (1,631)	NetBSD (255)
Security Tool (7,777)	OpenBSD (479)
Shell (3,103)	RedHat (12,469)

Shellcode (1,204)

Sniffer (886)

Slackware (941)

Solaris (1,607)

Spoof (2,166) SUSE (1,444) SQL Injection (16,102) Ubuntu (8,199) TCP (2,379) UNIX (9,159) Trojan (686) UnixWare (185) UDP (876) Windows (6,511) Virus (662) Other Vulnerability (31,136) Web (9,365) Whitepaper (3,729)



x86 (946) XSS (17,494)

Site Links About Us

News by Month History & Purpose Contact Information News Tags

Files by Month Terms of Service File Tags
File Directory Privacy Statement

Copyright Information

Hosting By Rokasec

Follow us on Twitter

