

	pucket storm										Search			
	what you dor													
Ī	Home	1	Files	Т	News	1	About	1	Contact	&[SERVICES_TAB]	Α	dd New	1	

Concrete 5 8.5.5 Phar Deserialization

Posted Jul 20, 2021

Concrete5 versions 8.5.5 suffer from a logging settings phar deserialization vulnerability. User input passed through the logFile request parameter is not properly sanitized before being used in a call to the file_exists() function at line 91. This can be exploited by malicious users to inject arbitrary PHP objects into the application scope (PHP Object Injection via phar:// stream wrapper), allowing them to carry out a variety of attacks, such as executing arbitrary PHP code. Successful exploitation of this vulnerability requires an administrator account.

tags | advisory, arbitrary, php advisories | CVE-2021-36766 Share This LinkedIn Reddit Digg StumbleUpon Lik€ TWEE

Change Mirror	Download
Concrete5 <= 8.5.5 (Logging Settings) Phar Deserialization Vulnerability	
[-] Software Link:	
https://www.concrete5.org	
[-] Affected Versions:	
Version 8.5.5 and prior versions.	
[-] Vulnerability Description:	
The vulnerable code is located within the /concrete/controllers/single_page/dashboard/system/environment/logging.php script. Specifically, into the Logging:update_logging() method:	
<pre>61. public function update_logging() 62. {</pre>	
<pre>63. \$config = \$this->app->make('config'); 64. \$request = \$this->request;</pre>	
<pre>65. 66. if (!\$this->token->validate('update_logging')) { 67. return</pre>	
<pre>\$this->showError(\$this->token->getErrorMessage()); 68. }</pre>	
69. 70. // Load in variables from the request 71. \$mode = (string) \$request->request->get('logging_mode') === 'advanced' ? 'advanced' : 'simple' ? 72. \$handler = 'mode === 'simple' ? (string)	
<pre>\$request->request->get('handler', 'database') : null; 73. \$logFile = \$handler === 'file' ? (string)</pre>	
\$request->request->get('logFile') : null;	
\$request->request->get('enable dashboard_report') ? true : false; 75. \$logginglewel = strtoupper((string) \$request->request->get(logginglewel)');	
76. \$intLogErrorsPost = \$request->request->qet('ENABLE LOG ERRORS') === 1 ? 1 : 0;	
77. SintLogEmailsPost - \$request->request->get('ENABLE LOG_EMAILS') === 1 ? 1 : 0; 78. \$intLogAplPost = \$request->request->get('ENABLE LOG_API')	
=== 1 ? 1 : 0; 79.	
80. // Handle 'file' based logging 82. if (Shandler 'file') { 83. Sdirectory - dirname(GlogFile);	
84. 85.	
88. } 89. // Validate the file path, create the log file if needed	
91. if (!file_exists(\$logFile)) {	
User input passed through the "logfile" request parameter is not properly sanitized before being used in a call to the file exists() function at line 31. This can be exploited by malicious users to inject the same of the s	
[-] Solution:	
No official solution is currently available.	
[-] Disclosure Timeline:	
I20/12/2020] - Vendor notified through Hackerone I22/12/2020] - Vendor asks suggestions to fix the issue, feedback provided I18/03/2021] - Version 8.5.5 released, vulnerability not fixed I02/06/2021] - Asked for an update, no response I06/07/2021] - Asked for an update, no response I16/07/2021] - OVE number assigned I19/07/2021] - VUBI colliciosure Version 8.00 Version 8.00 Version 9.00	
[-] CVE Reference:	
The Common Vulnerabilities and Exposures project (cve.mitre.org) has assigned the name CVE-2021-36766 to this vulnerability.	
[-] Credits:	
Vulnerability discovered by Egidio Romano.	
[-] Other References:	
https://hackerone.com/reports/1063039	
[-] Original Advisory:	
http://karmainsecurity.com/KIS-2021-05	



File Archive: December 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
31					
Гор /	Autho	ors In	Last	30 D	ays

31	
Тор	Authors In Last 30 Days
Red H	at 157 files
Ubunt	tu 76 files
Liquio	Worm 23 files
Debia	n 21 files
nu11s	ecur1ty 11 files
malvu	In 11 files
Gento	O 9 files
Goog	le Security Research 8 files
Julien	Ahrens 4 files
T. Wel	ber 4 files

File Tags File Archives ActiveX (932) December 2022 Advisory (79,754) Arbitrary (15,694) October 2022 BBS (2.859) September 2022 August 2022 Bypass (1,619) 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) Magazine (586) FreeBSD (1.242) Gentoo (4.272) Perl (1.418) 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) Mac OS X (684) Ruby (594) Mandriva (3,105) Scanner (1.631) Security Tool (7,777) OpenBSD (479) RedHat (12,469) Shellcode (1,204)

Solaris (1,607)

Sniffer (886)

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

