# SuiteCRM 7.11.10 SQL Injection

Authored by EgiX | Site karmainsecurity.com

Posted Feb 13, 2020

SuiteCRM versions 7.11.10 and below suffer from multiple remote SQL injection vulnerabilities.

tags | exploit, remote, vulnerability, sql injection
advisories | CVE-2020-8804
SHA-256 | 6d0664ee294d9c0e355362341a51a1fb0526746a2bbe5d841ef37520620739c4 Download | Favorite | View

Related Files



Change Mirror Download

```
------------------------------------------------------------
SuiteCRM <= 7.11.10 Multiple SQL Injection Vulnerabilities
------------------------------------------------------------


[-] Software Link:

https://suitecrm.com/


[-] Affected Versions:

Version 7.11.10 and prior versions.


[-] Vulnerabilities Description:

1) The vulnerability is located within the SOAP API, specifically into
the set_entries() SOAP
function. User input passed through the "name_value_lists" parameter
(specifically the "first_name"
and "last_name" elements) isn't properly sanitized before being used to
construct a SQL query from
within the check_for_duplicate_contacts() function. This can be
exploited by malicious users to e.g.
read sensitive data from the database through in-bound SQL injection
attacks.

2) The vulnerability is located within the EmailUIAjax interface. User
input passed through the
"bean_module" and "bean_id" parameters when handling the "addContact"
action isn't properly sanitized
before being used to construct a SQL query. This can be exploited by
malicious users to read sensitive
data from the database through boolean-based SQL injection attacks.

3) The vulnerability is located within the EmailUIAjax interface. User
input passed through the
"contactData" parameter when handling the "addContactsMultiple" action
isn't properly sanitized
before being used to construct a SQL query. This can be exploited by
malicious users to read
sensitive data from the database through boolean-based SQL injection
attacks.

4) The vulnerability is located within the EmailUIAjax interface. User
input passed through the "ids"
parameter when handling the "removeContact" action isn't properly
sanitized before being used to
construct a SQL query. This can be exploited by malicious users to read
sensitive data from the database
through time-based SQL injection attacks.

5) The vulnerability is located within the MailMerge module. User input
passed through the "rel_module"
parameter when handling the "search" action isn't properly sanitized
before being used to construct a
SQL query. This can be exploited by malicious users to read sensitive
data from the database through
time-based SQL injection attacks.


[-] Solution:

Upgrade to version 7.11.11 or later.


[-] Disclosure Timeline:

[19/09/2019] - Vendor notified
[20/09/2019] - Vendor acknowledgement
[12/11/2019] - Vendor contacted again asking for updates, no response
[20/01/2020] - Vendor notified about public disclosure intention, no
response
[07/02/2020] - CVE number assigned
[10/02/2020] - Version 7.11.11 released
[12/02/2020] - Public disclosure


[-] CVE Reference:

The Common Vulnerabilities and Exposures project (cve.mitre.org)
has assigned the name CVE-2020-8804 to these vulnerabilities.


[-] Credits:

Vulnerabilities discovered by Egidio Romano.


[-] Original Advisory:

http://karmainsecurity.com/KIS-2020-05
```





## 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