SugarCRM Cross Site Scripting

Authored by EgiX

Posted Aug 12, 2020

SugarCRM versions prior to 10.1.10 suffer from multiple cross site scripting vulnerabilities.

tags | exploit, vulnerability, xss
advisories | CVE-2020-17372
SHA-256 | 3b4dd8343f28746f3b059b1453af1a6567db0f415690776d8a7b2d7da1d2f3d9 **Download** | **Favorite** | **View**

Related Files

Share This

Like Twee LinkedIn Reddit Digg StumbleUpon

Change Mirror Download

```
SugarCRM < 10.1.0 Multiple Reflected Cross-Site Scripting Vulnerabilities

*• Software Link:*

https://www.sugarcrm.com/

*• Affected Versions:*

All versions prior to 10.1.0 (Q3 2020).

*• Vulnerabilities Description:*

1) User input passed through the “do” parameter when action is set to
“metadata” is not properly sanitized before being used to generate HTML
output. This can be exploited by malicious users to carry out Reflected
Cross-Site Scripting (XSS) attacks.

*• Proof of Concept 1:*

https://[HOST]/index.php?action=metadata&do=%27);alert(%27XSS%27)//

2) User input passed through the “current_step” parameter to the “Reports”
module is not properly sanitized before being used to generate HTML output.
This can be exploited by malicious users to carry out Reflected Cross-Site
Scripting (XSS) attacks.

*• Proof of Concept 2:*

https://
[HOST]/index.php?
module=Reports&action=ReportsWizard&save_report=on&current_step=%22%3E%3Cimg%20src=x%20onerror=alert(%22XSS%22)

3) User input passed through the “updated_records” parameter is not
properly sanitized before being used to generate HTML output. This can be
exploited by malicious users to carry out Reflected Cross-Site Scripting
(XSS) attacks.

*• Proof of Concept 3:*

https://
[HOST]/index.php?updated_records=%3Cimg%20src=x%20onerror=alert(/XSS/)%3E

*• Solution:*

Upgrade to version 10.1.0 (Q3 2020) or later.

*• Disclosure Timeline:*

[05/02/2020] - Vendor notified
[06/02/2020] - Automoatic vendor response received
[26/03/2020] - Vendor contacted again; no response
[17/04/2020] - Vendor contacted again; no response
[18/06/2020] - Vendor nodified 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-2020-17372
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=2020-17372> to these
vulnerabilities.

*• Credits:*

Vulnerabilities discovered by Egidio Romano.
```

Login or Register to add favorites

Follow us on Twitter

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

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

packet storm

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