SugarCRM < 10.1.0 (Reports Export) SQL Injection Vulnerability

From: Egidio Romano <n0b0d13s () gmail com>
Date: Mon, 10 Aug 2020 16:31:29 +0200

```
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

*• 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.
```


By Date By Thread

Current thread:

SugarCRM < 10.1.0 (Reports Export) SQL Injection Vulnerability ***Egidio Romano (Aug 11)***