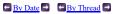


# <u>Full Disclosure</u> mailing list archives



List Archive Search



## 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:\*

\*• 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:\*

\*• Solution:\*

Upgrade to version 10.1.0 (Q3 2020) or later.

\*• Disclosure Timeline:\*

[05/02/2020] - Vendor notified [05/02/2020] - 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 <a href="http://cve.mitre.org/cqi-bin/cvename.cqi?name=2020-17373">http://cve.mitre.org/cqi-bin/cvename.cqi?name=2020-17373</a> to this vulnerability.

\* · Credits · \*

Vulnerability discovered by Egidio Romano.

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



### Current thread:

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

**Nmap Security** Npcap packet Security Lists Security Tools Scanner capture Nmap Announce Vuln scanners About/Contact User's Guide Ref Guide Nmap Dev Password audit Privacy Install Guide API docs Full Disclosure Web scanners Advertising Docs Download Open Source Security Nmap Public Source License Wireless Download Npcap OEM BreachExchange Exploitation Nmap OEM