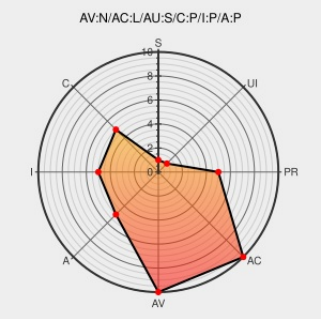
CVE-2014-5462

Published on: 12/08/2014 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:53 PM UTC

CVE-2014-5462

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Openemr from Open-emr contain the following vulnerability:

Multiple SQL injection vulnerabilities in OpenEMR 4.1.2 (Patch 7) and earlier allow remote authenticated users to execute arbitrary SQL commands via the (1) layout_id parameter to interface/super/edit_layout.php; (2) form_patient_id, (3) form_drug_name, or (4) form_lot_number parameter to interface/reports/prescriptions_report.php; (5) payment_id parameter to interface/billing/edit_payment.php; (6) id parameter to interface/forms_admin/forms_admin.php; (7) form_pid or (8) form_encounter parameter to interface/billing/sl_eob_search.php; (9) sortby parameter to interface/logview/logview.php; form_facility parameter to (10) procedure_stats.php, (11) pending_followup.php, or (12) pending_orders.php in interface/orders/; (13) patient, (14) encounterid, (15) formid, or (16) issue parameter to interface/patient_file/deleter.php; (17) search_term parameter to interface/patient_file/encounter/coding_popup.php; (18) text parameter to interface/patient_file/encounter/search_code.php; (19) form_addr1, (20) form_addr2, (21) form_attn, (22) form_country, (23) form_freeb_type, (24) form_partner, (25) form_name, (26) form_zip, (27) form_state, (28) form_city, or (29) form_cms_id parameter to interface/practice/ins_search.php; (30) form_pid parameter to interface/patient_file/problem_encounter.php; (31) patient, (32) form_provider, (33) form_apptstatus, or (34) form_facility parameter to interface/reports/appointments_report.php; (35) db_id parameter to interface/patient_file/summary/demographics_save.php; (36) p parameter to interface/fax/fax_dispatch_newpid.php; or (37) patient_id parameter to interface/patient_file/reminder/patient_reminders.php.

CVE-2014-5462 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 6.5 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE

Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Full Disclosure: CVE-2014-5462 - Multiple Authenticated SQL Injections In OpenEMR	Exploit seclists.org text/html	FULLDISC 20141205 CVE-2014-5462 - Multiple Authenticated SQL Injections In OpenEMR
cve-2014-5462 - Portcullis	Exploit www.portcullis-security.com text/html	MISC www.portcullis-security.com/security-research-and-downloads/security-advisories/cve-2014-5462/
OpenEMR v5_0_1_4: SQL Injection in interface/logview/logview.php · Issue #1782 · openemr/openemr · GitHub	github.com text/html	CONFIRM github.com/openemr/openemr/issues/1782
OpenEMR 4.1.2(7) SQL Injection ≈ Packet Storm	Exploit packetstormsecurity.com text/html	MISC packetstormsecurity.com/files/129403/OpenEMR-4.1.2-7-SQL-Injection.html

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Open-emr	Openemr	All	patch_7	All	All

cpe:2.3:a:open-emr:openemr:*:patch_7:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→