Authenticated SQL Injection in Koha displayby parameter of suggestion.pl

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2026-31844
State	PUBLISHED
Assigner	TuranSec
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-03-11 07:16:43 UTC
Updated	2026-05-07 18:27:42 UTC
Description	An authenticated SQL Injection vulnerability (CWE-89) exists in the Koha staff interface in the /cgi-bin/koha/suggestion/sug

Risk And Classification

Primary CVSS: v4.0 8.7 HIGH from 309f9ea4-e3e9-4c6c-b79d-e8eb01244f2c

CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

Problem Types: CWE-89 | CWE-89 CWE-89 Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

Version	Source	Type	Score	Severity	Vector
4.0	309f9ea4-e3e9-4c6c-b79d-e8eb01244f2c	Secondary	8.7	HIGH	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H
4.0	CNA	CVSS	8.7	HIGH	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H
3.1	309f9ea4-e3e9-4c6c-b79d-e8eb01244f2c	Secondary	8.8	HIGH	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
3.1	CNA	CVSS	8.8	HIGH	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
2.0	309f9ea4-e3e9-4c6c-b79d-e8eb01244f2c	Secondary	9		AV:N/AC:L/Au:S/C:C/I:C/A:C
2.0	CNA	CVSS	9		AV:N/AC:L/Au:S/C:C/I:C/A:C

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

Low

User Interaction

None

Confidentiality

High

Integrity

High

Availability

High

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

Single

Confidentiality

Complete

Integrity

Complete

Availability

Complete

AV:N/AC:L/Au:S/C:C/I:C/A:C

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Koha	Koha	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Koha Community	Koha	affected 24.11.0 24.11.12 semver	Linux
CNA	Koha Community	Koha	affected 25.05.0 25.05.07 semver	Linux
CNA	Koha Community	Koha	affected 25.11.0 25.11.01 semver	Linux

References

Reference	Source	Link	Tags
bugs.koha-community.org/bugzilla3/show_bug.cgi	309f9ea4-e3e9-4c6c-b79d-e8eb01244f2c	bugs.koha-community.org	Issue
koha-community.gitlab.io/KohaAdvent/2025-12-09-security-all	309f9ea4-e3e9-4c6c-b79d-e8eb01244f2c	koha-community.gitlab.io	Not A
koha-community.org/koha-25-11-01-released	309f9ea4-e3e9-4c6c-b79d-e8eb01244f2c	koha-community.org	Rele
CVE Program record	CVE.ORG	www.cve.org	canc
NVD vulnerability detail	NVD	nvd.nist.gov	canc

Vendor Comments And Credit

Discovery Credit

CNA: Raximov Shukrulloh (Mothra) (en)

There are currently no legacy QID mappings associated with this CVE.

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report