WordPress xPromoter plugin <= 1.3.4 - SQL Injection vulnerability

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

Summary

CVE	CVE-2025-68053
State	PUBLISHED
Assigner	Patchstack
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-12-16 09:16:00 UTC
Updated	2026-04-27 19:16:23 UTC
Description	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in LambertGroup xPro

Risk And Classification

Primary CVSS: v3.1 8.5 HIGH from audit@patchstack.com

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

EPSS: 0.000590000 probability, percentile 0.182280000 (date 2026-04-27)

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

Version	Source	Type	Score	Severity	Vector
3.1	audit@patchstack.com	Secondary	8.5	HIGH	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:L
3.1	CNA	CVSS	8.5	HIGH	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:L

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Changed

Confidentiality

High

ntegrity

None

Availability

Low

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	LambertGroup	XPromoter	affected 1.3.4 custom	Not specified

References

Reference	Source	Link	Tags
patchstack.com/database/Wordpress/Plugin/top_bar_promoter/vulnerability/word...	audit@patchstack.com	patchstack.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, a

Vendor Comments And Credit

Discovery Credit

CNA: Phat RiO | Patchstack Bug Bounty Program (en)

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