



WordPress Paytm Payment Gateway Plugin <= 2.7.3 is vulnerable to SQL Injection

MITRE

NVD

CVE.ORG

JSON API

Print: PDF

Summary

CVE	CVE-2022-45805
State	PUBLISHED
Assigner	Patchstack
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-11-03 13:15:08 UTC
Updated	2026-04-28 19:19:01 UTC

Description Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Paytm Paytm Payr

Risk And Classification

Primary CVSS: v3.1 9.8 CRITICAL from nvd@nist.gov

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

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
3.1	nvd@nist.gov	Primary	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
3.1	ADP	DECLARED	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
3.1	audit@patchstack.com	Secondary	8.2	HIGH	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:L/A:L
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
3.1	CNA	CVSS	8.2	HIGH	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:L/A:L

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope
Unchanged

Confidentiality
High

Integrity
High

Availability
High

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



NVD Known Affected Configurations (CPE 2.3)						
Type	Vendor	Product	Version	Update	Edition	Language
Application	Paytm	Payment Gateway	All	All	All	All

Vendor Declared Affected Products				
Source	Vendor	Product	Version	Platforms
CNA	Paytm	Paytm Payment Gateway	affected n/a 2.7.3 custom	Not specified
ADP	Paytm	Payment Gateway	affected 2.7.3 custom	Not specified

References	
Reference	Source
WordPress Paytm Payment Gateway plugin <= 2.7.3 - Auth. SQL Injection (SQLi) vulnerability - Patchstack	af854a3a-2127-422b-91ae-364c
patchstack.com/database/Wordpress/Plugin/paytm-payments/vulnerability/wordpr...	MITRE
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD



Vendor Comments And Credit
Discovery Credit
CNA: Aman Rawat (Patchstack Alliance) (en)

Additional Advisory Data
Solutions
CNA: Update to 2.7.7 or a higher version.

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

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)