



# WordPress Super Store Finder plugin <= 6.9.7 - SQL Injection vulnerability

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2024-43976
<b>State</b>	PUBLISHED
<b>Assigner</b>	Patchstack
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2024-09-17 23:15:18 UTC
<b>Updated</b>	2026-04-01 16:17:47 UTC
<b>Description</b>	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in highwarden Super S

## 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 Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

## 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	<a href="#">Superstorefinder</a>	<a href="#">Super Store Finder</a>	All	All	All	All

  

Vendor Declared Affected Products				
Source	Vendor	Product	Version	Platforms
CNA	<a href="#">Highwarden</a>	<a href="#">Super Store Finder</a>	affected 6.9.7 custom	Not specified
ADP	<a href="#">Superstorefinder</a>	<a href="#">Super Store Finder</a>	affected 6.9.7 custom	Not specified

  

References			
Reference	Source	Link	Tags
<a href="#">patchstack.com/database/Wordpress/Plugin/superstorefinder-wp/vulnerability/w...</a>	<a href="mailto:audit@patchstack.com">audit@patchstack.com</a>	<a href="#">patchstack.com</a>	
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>	canonical, and

  

Vendor Comments And Credit
Discovery Credit
<b>CNA: Bonds   Patchstack Bug Bounty Program (en)</b>

  

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](https://cve.report/api)

CVE.report and Source URL Uptime Status [status.cve.report](https://status.cve.report)