



# Superb slideshow gallery <= 13.1 - Authenticated (Subscriber+) SQL Injection via Shortcode

[MITRE](#)

[NVD](#)

[CVE.ORG](#)

[JSON API](#)

[Print: PDF](#)

| Summary         |                                                                                                                                     |
|-----------------|-------------------------------------------------------------------------------------------------------------------------------------|
| CVE             | CVE-2023-5434                                                                                                                       |
| State           | PUBLISHED                                                                                                                           |
| Assigner        | Wordfence                                                                                                                           |
| Source Priority | CVE Program / NVD first with legacy fallback                                                                                        |
| Published       | 2023-10-31 09:15:08 UTC                                                                                                             |
| Updated         | 2026-04-08 18:18:28 UTC                                                                                                             |
| Description     | The Superb slideshow gallery plugin for WordPress is vulnerable to SQL Injection via the plugin's shortcode in versions up to 13.1. |

Risk And Classification

Primary CVSS: v3.1 6.5 MEDIUM from nvd@nist.gov

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

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   | 6.5   | MEDIUM   | CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N |
| 3.1     | security@wordfence.com | 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                    | DECLARED  | 8.8   | HIGH     | CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H |

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

None

High

Integrity

None

Availability

None

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



NVD Known Affected Configurations (CPE 2.3)

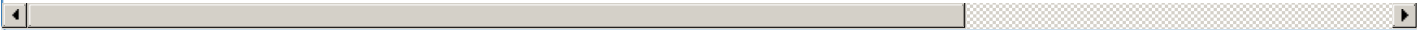
| Type        | Vendor | Product                  | Version | Update | Edition | Language |
|-------------|--------|--------------------------|---------|--------|---------|----------|
| Application | Gopius | Superb Slideshow Gallery | All     | All    | All     | All      |

Vendor Declared Affected Products

| Source | Vendor | Product                  | Version              | Platforms     |
|--------|--------|--------------------------|----------------------|---------------|
| CNA    | Gopius | Superb Slideshow Gallery | affected 13.1 semver | Not specified |

References

| Reference                                                                                  | Source                               | Link |
|--------------------------------------------------------------------------------------------|--------------------------------------|------|
| 403 Forbidden                                                                              | af854a3a-2127-422b-91ae-364da2661108 | pl   |
| Superb slideshow gallery <= 13.1 - Authenticated (Subscriber+) SQL Injection via Shortcode | af854a3a-2127-422b-91ae-364da2661108 | w    |
| 403 Forbidden                                                                              | af854a3a-2127-422b-91ae-364da2661108 | pl   |
| CVE Program record                                                                         | CVE.ORG                              | w    |
| NVD vulnerability detail                                                                   | NVD                                  | n'   |



Vendor Comments And Credit

Discovery Credit  
**CNA:** István Márton (en)

Additional Advisory Data

| Source | Time                     | Event           |
|--------|--------------------------|-----------------|
| CNA    | 2023-10-05T00:00:00.000Z | Discovered      |
| CNA    | 2023-10-07T00:00:00.000Z | Vendor Notified |
| CNA    | 2023-10-30T00:00:00.000Z | Disclosed       |

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

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)