



# Appointment Booking Calendar <= 1.6.10.6 - Unauthenticated Arbitrary Appointment View, Modification and Deletion

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

## Summary

<b>CVE</b>	CVE-2026-4807
<b>State</b>	PUBLISHED
<b>Assigner</b>	Wordfence
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-05-07 03:16:08 UTC
<b>Updated</b>	2026-05-07 03:16:08 UTC
<b>Description</b>	The Appointment Booking Calendar plugin for WordPress is vulnerable to Missing Authorization in versions up to and includ

## Risk And Classification

**Primary CVSS:** v3.1 6.5 MEDIUM from security@wordfence.com

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

**Problem Types:** CWE-862 | CWE-862 CWE-862 Missing Authorization

Version	Source	Type	Score	Severity	Vector
3.1	security@wordfence.com	Primary	6.5	MEDIUM	<b>CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:L</b>
3.1	CNA	DECLARED	6.5	MEDIUM	<b>CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:L</b>

## CVSS v3.1 Breakdown

Attack Vector

**Network**

Attack Complexity

**Low**

Privileges Required

**None**

User Interaction

**None**

Scope

**Unchanged**

Confidentiality

**None**

Integrity

Low

Availability

Low

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

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platform
CNA	Croixhaug	Appointment Booking Calendar Simply Schedule Appointments Booking Plugin	affected 1.6.10.6 semver	Not spec

### References

Reference	Source	Link
plugins.trac.wordpress.org/browser/simply-schedule-appointments/tags/1.6.9.29/booking-ap...	security@wordfence.com	plugins.trac.word
plugins.trac.wordpress.org/changeset/3511993/simply-schedule-appointments/trunk/includes	security@wordfence.com	plugins.trac.word
plugins.trac.wordpress.org/browser/simply-schedule-appointments/tags/1.6.9.29/includes/l...	security@wordfence.com	plugins.trac.word
plugins.trac.wordpress.org/browser/simply-schedule-appointments/tags/1.6.9.29/includes/c...	security@wordfence.com	plugins.trac.word
plugins.trac.wordpress.org/browser/simply-schedule-appointments/tags/1.6.9.29/includes/c...	security@wordfence.com	plugins.trac.word
plugins.trac.wordpress.org/browser/simply-schedule-appointments/tags/1.6.9.29/includes/c...	security@wordfence.com	plugins.trac.word
plugins.trac.wordpress.org/browser/simply-schedule-appointments/tags/1.6.9.29/includes/l...	security@wordfence.com	plugins.trac.word
www.wordfence.com/threat-intel/vulnerabilities/id/436ab843-7729-4d57-9c9e-2ede2...	security@wordfence.com	www.wordfence.c
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

### Vendor Comments And Credit

Discovery Credit

**CNA:** Athiwat Tiprasaharn (en)

### Additional Advisory Data

Source	Time	Event
CNA	2026-03-25T12:43:44.000Z	Vendor Notified
CNA	2026-05-06T13:33:55.000Z	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](#)

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