



# LatePoint Plugin <= 4.9.9 - Missing Authorization and Sensitive Information Exposure via IDOR

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

## Summary

<b>CVE</b>	CVE-2024-2472
<b>State</b>	PUBLISHED
<b>Assigner</b>	Wordfence
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2024-06-14 10:15:09 UTC
<b>Updated</b>	2026-04-08 18:21:06 UTC
<b>Description</b>	The LatePoint Plugin plugin for WordPress is vulnerable to unauthorized access of data and modification of data due to a r

## Risk And Classification

**Primary CVSS:** v3.1 9.1 CRITICAL from security@wordfence.com

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

**Problem Types:** CWE-639 | CWE-639 CWE-639 Authorization Bypass Through User-Controlled Key

Version	Source	Type	Score	Severity	Vector
3.1	security@wordfence.com	Secondary	9.1	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N
3.1	CNA	DECLARED	9.1	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

None

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

### NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Latepoint	Latepoint	All	All	All	All

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Latepoint	LatePoint Plugin	affected 4.9.9 semver	Not specified
ADP	Latepoint	Latepoint Plugin	affected 4.9.9.1 custom	Not specified

### References

Reference	Source	Link
www.wordfence.com/threat-intel/vulnerabilities/id/6215fa9f-06bc-4dc8-b1f5-a3bb7...	af854a3a-2127-422b-91ae-364da2661108	<a href="http://www.wordfence.com/threat-intel/vulnerabilities/id/6215fa9f-06bc-4dc8-b1f5-a3bb7...">www.wordfence.com/threat-intel/vulnerabilities/id/6215fa9f-06bc-4dc8-b1f5-a3bb7...</a>
websec.nl/blog/critical-idor-vulnerability-in-latepoint-plugin-exposes-...	security@wordfence.com	<a href="http://websec.nl/blog/critical-idor-vulnerability-in-latepoint-plugin-exposes-...">websec.nl/blog/critical-idor-vulnerability-in-latepoint-plugin-exposes-...</a>
aramhairchitects.nl	af854a3a-2127-422b-91ae-364da2661108	<a href="http://aramhairchitects.nl">aramhairchitects.nl</a>
wpdocs.latepoint.com/changelog	af854a3a-2127-422b-91ae-364da2661108	<a href="http://wpdocs.latepoint.com/changelog">wpdocs.latepoint.com/changelog</a>
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>

### Vendor Comments And Credit

Discovery Credit

**CNA:** Gharib Sharifi (en)

**CNA:** Joel Aviad Ossi (en)

### Additional Advisory Data

Source	Time	Event
CNA	2024-06-13T21:00:45.000Z	Disclosed

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

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)