



# WordPress Atarim plugin <= 4.2.1 - Sensitive Data Exposure vulnerability

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

## Summary

<b>CVE</b>	CVE-2025-60188
<b>State</b>	PUBLISHED
<b>Assigner</b>	Patchstack
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2025-11-06 16:16:03 UTC
<b>Updated</b>	2026-04-01 15:17:45 UTC
<b>Description</b>	Insertion of Sensitive Information Into Sent Data vulnerability in Vito Peleg Atarim atarim-visual-collaboration allows Retrieval of Sensitive Information

## Risk And Classification

**Primary CVSS:** v3.1 7.5 HIGH from ADP

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

**EPSS:** 0.055010000 probability, percentile 0.901870000 (date 2026-04-02)

**Problem Types:** CWE-201 | CWE-201 Insertion of Sensitive Information Into Sent Data

Version	Source	Type	Score	Severity	Vector
3.1	ADP	DECLARED	7.5	HIGH	CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	7.5	HIGH	CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

High

Privileges Required

None

User Interaction

Required

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

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

#### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Vito Peleg	Atarim	affected 4.2.1 custom	Not specified

#### References

Reference	Source	Link
patchstack.com/database/Wordpress/Plugin/atarim-visual-collaboration/vulnera...	audit@patchstack.com	patchstack.co
github.com/m4sh-wacker/CVE-2025-60188-Atarim-Plugin-Exploit	134c704f-9b21-4f2e-91b3-4a467353bcc0	github.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

#### Vendor Comments And Credit

Discovery Credit

**CNA:** Denver Jackson | Patchstack Bug Bounty Program (en)

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](#).

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