WordPress Image Source Control Plugin <= 2.17.0 is vulnerable to Sensitive Data Exposure

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2023-52187
State	PUBLISHED
Assigner	Patchstack
Source Priority	CVE Program / NVD first with legacy fallback
Published	2024-01-27 00:15:24 UTC
Updated	2026-04-28 19:23:01 UTC
Description	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Thomas Maier Image Source Control Lite – Sho

Risk And Classification

Primary CVSS: v3.1 7.5 HIGH from nvd@nist.gov

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

EPSS: 0.002820000 probability, percentile 0.514910000 (date 2026-04-28)

Problem Types: CWE-200 | NVD-CWE-noinfo | CWE-200 CWE-200 Exposure of Sensitive Information to an Unauthorized Actor

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	7.5	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
3.1	audit@patchstack.com	Secondary	5.3	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N
3.1	CNA	CVSS	5.3	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

None

Availability

None

CVSS:3.1/AV:N/AC:L/PR:N/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	Imagesourcecontrol	Image Source Control	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Thomas Maier	Image Source Control Lite Show Image Credits And Captions	affected n/a 2.17.0 custom	Not specified

References

Reference	Source
WordPress Image Source Control Lite plugin <= 2.17.0 - Sensitive Data Exposure via Log File vulnerability - Patchstack	af854a3a-2127-422
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

Vendor Comments And Credit

Discovery Credit

CNA: Joshua Chan (Patchstack Alliance) (en)

Additional Advisory Data

Solutions

CNA: Update to 2.17.1 or a higher version.

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

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**