Seeyon Zhiyuan OA System Path Traversal File Upload

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

Summary

CVE	CVE-2025-34040
State	PUBLISHED
Assigner	VulnCheck
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-06-24 02:15:22 UTC
Updated	2026-04-29 20:16:28 UTC
Description	An arbitrary file upload vulnerability exists in the Zhiyuan OA platform via the wpsAssistServlet interface. The realFileType a

Risk And Classification

Primary CVSS: v4.0 10 CRITICAL from disclosure@vulncheck.com

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

EPSS: 0.148330000 probability, percentile 0.945380000 (date 2026-05-04)

Problem Types: CWE-22 | CWE-434 | CWE-434 CWE-434 Unrestricted Upload of File with Dangerous Type | CWE-22 CWE-22 Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

Version	Source	Type	Score	Severity	Vector
4.0	disclosure@vulncheck.com	Secondary	10	CRITICAL	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/S
4.0	CNA	CVSS	10	CRITICAL	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/S

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

None

User Interaction

None

Confidentiality

High

Integrity

High

Availability

High

Sub Conf.

High

Sub Integrity

High

Sub Availability

High

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platform
CNA	Seeyon Beijing Zhiyuan Internet Software Co. Ltd.	Zhiyuan OA Web Application System	affected 5.0 semver	Not speci
CNA	Seeyon Beijing Zhiyuan Internet Software Co. Ltd.	Zhiyuan OA Web Application System	affected 5.1 5.6sp1 custom	Not speci
CNA	Seeyon Beijing Zhiyuan Internet Software Co. Ltd.	Zhiyuan OA Web Application System	affected 6.0 6.1sp2 custom	Not speci
CNA	Seeyon Beijing Zhiyuan Internet Software Co. Ltd.	Zhiyuan OA Web Application System	affected 7.0 semver	Not speci
CNA	Seeyon Beijing Zhiyuan Internet Software Co. Ltd.	Zhiyuan OA Web Application System	affected 7.0sp1 7.1 custom	Not speci
CNA	Seeyon Beijing Zhiyuan Internet Software Co. Ltd.	Zhiyuan OA Web Application System	affected 7.1sp1 custom	Not speci
CNA	Seeyon Beijing Zhiyuan Internet Software Co. Ltd.	Zhiyuan OA Web Application System	affected 8.0 8.0sp2 custom	Not speci

References

Reference	Source	Link
www.cnblogs.com/pursue-security/p/17677130.html	disclosure@vulncheck.com	www.cnblogs.com
www.cnvd.org.cn/flaw/show/CNVD-2021-01627	disclosure@vulncheck.com	www.cnvd.org.cn
vulncheck.com/advisories/zhiyuan-oa-system-path-traversal-file-upload	disclosure@vulncheck.com	vulncheck.com
www.exploit-db.com/exploits/52490	af854a3a-2127-422b-91ae-364da2661108	www.exploit-db.com
service.seeyon.com/patchtools/tp.html	disclosure@vulncheck.com	service.seeyon.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

Vendor Comments And Credit

Discovery Credit

CNA: Pursue Security (en)

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**