Weaver E-cology 9.5 Unauthenticated Arbitrary File Read via XmlRpcServlet

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

Summary

CVE	CVE-2022-50992
State	PUBLISHED
Assigner	VulnCheck
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-30 17:16:24 UTC
Updated	2026-04-30 17:19:57 UTC
Description	Weaver (Fanwei) E-cology 9.5 versions prior to 10.52 contain an arbitrary file read vulnerability in the XmlRpcServlet interfa

Risk And Classification

Primary CVSS: v4.0 8.7 HIGH from disclosure@vulncheck.com

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N/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: 0.001220000 probability, percentile 0.306680000 (date 2026-05-05)

Problem Types: CWE-22 | 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	8.7	HIGH	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA
4.0	CNA	CVSS	8.7	HIGH	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA
3.1	disclosure@vulncheck.com	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	CNA	CVSS	7.5	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

None

User Interaction

None

Confidentiality

High

Integrity

None

Availability

None

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N/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

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Weaver Network Co. Ltd.	E-cology	affected 10.52 custom	Not specified

References

Reference	Source	Link	Ta
blog.csdn.net/qq_36618918/article/details/135104295	disclosure@vulncheck.com	blog.csdn.net	
www.weaver.com.cn/cs/ecology_full_log.html	disclosure@vulncheck.com	www.weaver.com.cn	
blog.csdn.net/xiayu729100940/article/details/135205082	disclosure@vulncheck.com	blog.csdn.net	
www.weaver.com.cn/cs/securityDownload.html	disclosure@vulncheck.com	www.weaver.com.cn	
www.cnvd.org.cn/flaw/show/CNVD-2022-43245	disclosure@vulncheck.com	www.cnvd.org.cn	
www.vulncheck.com/advisories/weaver-e-cology-unauthenticated-arbitrary-file-rea...	disclosure@vulncheck.com	www.vulncheck.com	
CVE Program record	CVE.ORG	www.cve.org	ca
NVD vulnerability detail	NVD	nvd.nist.gov	ca

Vendor Comments And Credit

Discovery Credit

CNA: The Shadowserver Foundation (en)

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