



Weaver E-cology 10.0 Unauthenticated RCE via dubboApi Debug Endpoint

MITRE

NVD

CVE.ORG

JSON API

Print: PDF

Summary	
CVE	CVE-2026-22679
State	PUBLISHED
Assigner	VulnCheck
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-07 13:16:45 UTC
Updated	2026-05-05 14:16:07 UTC
Description	Weaver (Fanwei) E-cology 10.0 versions prior to 20260312 contain an unauthenticated remote code execution vulnerability

Risk And Classification

Primary CVSS: v4.0 9.3 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: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/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

EPSS: 0.001810000 probability, percentile 0.393300000 (date 2026-05-05)

Problem Types: CWE-306 | CWE-306 CWE-306 Missing Authentication for Critical Function

Version	Source	Type	Score	Severity	Vector
4.0	disclosure@vulncheck.com	Secondary	9.3	CRITICAL	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/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/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X
4.0	CNA	CVSS	9.3	CRITICAL	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/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/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X
3.1	disclosure@vulncheck.com	Secondary	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
3.1	CNA	CVSS	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

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.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/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/MSG: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

High

Availability

High

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Weaver	E-cology	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Weaver Network Co. Ltd.	E-cology	affected 20260312 date	Not specified
References				
Reference		Source		Link
www.vulncheck.com/advisories/weaver-e-cology-unauthenticated-rce-via-dubboapi-d...		disclosure@vulncheck.com		www.vulncheck.com
ti.qianxin.com/vulnerability/notice-detail/1760		disclosure@vulncheck.com		ti.qianxin.com
blog.vega.io/posts/cve-2026-22679-weaver-ecology-exploitation		134c704f-9b21-4f2e-91b3-4a467353bcc0		blog.vega.io
www.weaver.com.cn/cs/securityDownload.html		disclosure@vulncheck.com		www.weaver.com.cn
h4cker.zip/post/d5d211		disclosure@vulncheck.com		h4cker.zip
CVE Program record		CVE.ORG		www.cve.org
NVD vulnerability detail		NVD		nvd.nist.gov
Vendor Comments And Credit				
Discovery Credit				
CNA: The Shadowserver Foundation (en)				
There are currently no legacy QID mappings associated with this CVE.				