Advantech WISE-DeviceOn Server < 5.4 Hard-coded JWT Key Authentication Bypass

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

Summary

CVE	CVE-2025-34256
State	PUBLISHED
Assigner	VulnCheck
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-12-05 18:15:55 UTC
Updated	2026-04-15 19:16:32 UTC
Description	Advantech WISE-DeviceOn Server versions prior to 5.4 contain a hard-coded cryptographic key vulnerability. The product u

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: 0.002910000 probability, percentile 0.525390000 (date 2026-04-15)

Problem Types: CWE-321 | CWE-321 CWE-321 Use of Hard-coded Cryptographic Key

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
3.1	nvd@nist.gov	Primary	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.

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

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	Advantech	Wise-deviceon Server	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms

CNA	Advantech Co. Ltd.	WISE-DeviceOn Server	affected 5.4.0 semver	Not specified

References

Reference	Source	Link
www.vulncheck.com/advisories/advantech-wise-deviceon-server-hardcoded-jwt-key-a...	disclosure@vulncheck.com	www.v
advcloudfiles.advantech.com/cms/2ca1b071-fd78-4d7f-8a2a-7b4537a95d19/Security%20Advisory%...	disclosure@vulncheck.com	advclou
pellera.com/blog/advantech-wise-deviceon-cve-2025-34256-vulnerability	disclosure@vulncheck.com	pellera
docs.deviceon.advantech.com/docs/resource	disclosure@vulncheck.com	docs.d
CVE Program record	CVE.ORG	www.c
NVD vulnerability detail	NVD	nvd.nis

Vendor Comments And Credit

Discovery Credit

CNA: Alex Williams from Pellera Technologies (en)

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