



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

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2025-34256
<b>State</b>	PUBLISHED
<b>Assigner</b>	VulnCheck
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2025-12-05 18:15:55 UTC
<b>Updated</b>	2026-04-15 19:16:32 UTC
<b>Description</b>	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/MSX/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/MSX/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	Wise Deviceon Server	1.0-1.5.10	All

## References

Reference	Source	Link
<a href="http://www.vulncheck.com/advisories/advantech-wise-deviceon-server-hardcoded-jwt-key-a...">www.vulncheck.com/advisories/advantech-wise-deviceon-server-hardcoded-jwt-key-a...</a>	disclosure@vulncheck.com	<a href="http://www.vulncheck.com">www.vulncheck.com</a>
<a href="http://advcloudfiles.advantech.com/cms/2ca1b071-fd78-4d7f-8a2a-7b4537a95d19/Security%20Advisory%20-%202025-34256.pdf">advcloudfiles.advantech.com/cms/2ca1b071-fd78-4d7f-8a2a-7b4537a95d19/Security%20Advisory%20-%202025-34256.pdf</a>	disclosure@vulncheck.com	<a href="http://advcloudfiles.advantech.com">advcloudfiles.advantech.com</a>
<a href="https://pellerablog.com/blog/advantech-wise-deviceon-cve-2025-34256-vulnerability">pellerablog.com/blog/advantech-wise-deviceon-cve-2025-34256-vulnerability</a>	disclosure@vulncheck.com	<a href="https://pellerablog.com">pellerablog.com</a>
<a href="https://docs.deviceon.advantech.com/docs/resource">docs.deviceon.advantech.com/docs/resource</a>	disclosure@vulncheck.com	<a href="https://docs.deviceon.advantech.com">docs.deviceon.advantech.com</a>
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>

## Vendor Comments And Credit

### Discovery Credit

**CNA:** Alex Williams from Peller Technologies (en)

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

© CVE.report 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](https://www.mitre.org/licenses).

**Free CVE JSON API** [cve.report/api](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)