SQL Injection Vulnerability

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

Summary

CVE	CVE-2026-6888
State	PUBLISHED
Assigner	CSA
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-13 04:17:41 UTC
Updated	2026-05-13 16:17:02 UTC
Description	Successful exploitation of the SQL injection vulnerability could allow a remote authenticated attacker to execute arbitrary co

Risk And Classification

Primary CVSS: v3.1 7.2 HIGH from 5f57b9bf-260d-4433-bf07-b6a79e9bb7d4

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

EPSS: 0.000790000 probability, percentile 0.233220000 (date 2026-05-16)

Problem Types: CWE-89 | CWE-89 CWE-89 Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

Version	Source	Type	Score	Severity	Vector
3.1	5f57b9bf-260d-4433-bf07-b6a79e9bb7d4	Secondary	7.2	HIGH	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H
3.1	CNA	CVSS	7.2	HIGH	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

High

User Interaction

None

Scope

Unchanged

Confidentiality

High

ntegrity

High

Availability

High

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Advantech	SaaS Composer	affected prior to version 3.4.17	Not specified
CNA	Advantech	IoTSuite Growth Linux Docker	affected prior to version 2.2.0	Not specified
CNA	Advantech	IoTSuite Starter Linux Docker	affected prior to version 2.2.0	Not specified
CNA	Advantech	IoT Edge Linux Docker	affected prior to version 2.2.0	Not specified
CNA	Advantech	IoT Edge Windows	affected prior to version 2.2.0	Not specified
CNA	Advantech	WebAccess/SCADA	affected prior to version 9.2.3	Not specified
CNA	Advantech	WebAccess SaaS-Composer	affected prior to version 3.4.17.1	Not specified
CNA	Advantech	ECOWatch SaaS-Composer	affected prior to version 3.4.17	Not specified

References

Reference	Source	Link	Tags
www.csa.gov.sg/alerts-and-advisories/alerts/al-2026-050	5f57b9bf-260d-4433-bf07-b6a79e9bb7d4	www.csa.gov.sg	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

Vendor Comments And Credit

Discovery Credit

CNA: Hoa Ly Van Huu (en)

Additional Advisory Data

Solutions

CNA: Users and administrators of affected product versions are advised to update to the latest versions immediately. For SaaS Composer, IoTSuite Growth Linux docker, IoT Edge Windows, and ECOWatch please contact Advantech here https://wise-iot.advantech.com/en-tw/marketplace/help/technical-support for the official release of the fixed version. For IoTSuite Starter Linux docker, please refer to the update guide here https://portal-kbinsight-wiseiot-ensaas.practice.cloud.advantech.com/kb/library/detail/oPN5exOVNQq . As the update involves a reinstallation process, please refer to the reinstallation guide here https://portal-

kbinsight-wiseiot-ensaas.practice.cloud.advantech.com/kb/library/detail/JqNWAlMGz1JQ . For IoT Edge Linux docker, please refer to the update guide here https://portal-kbinsight-wiseiot-ensaas.practice.cloud.advantech.com/kb/library/detail/oPN5exOVNQq . As the update involves a reinstallation process, please refer to the reinstallation guide here https://portal-kbinsight-wiseiot-ensaas.practice.cloud.advantech.com/kb/library/detail/G0yWBn2mp2q . For WebAccess/SCADA and WebAccess SaaS-Composer, please refer to the update guide here https://www.advantech.com/en/support/details/installation .

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