ADVANTECH Enabling an Intelligent Planet

No. 1, Alley 20, Lane 26, Rueiguang Road,
Neihu District, Taipei 11491, Taiwan, R.O.C.
Tel: 886-2-2792-7818
Fax: 886-2-2218-3650

SECURITY ADVISORY

Vulnerabilities Identified in iView

Advantech iView v5.7.05_7057 or earlier versions failed to properly filter SNMP v1 trap (port 162) requests, a vulnerability that attackers could exploit to inject SQL commands.

Following a thorough investigation and confirmation of these issues, Advantech has released an update, iView v5.8.01_7109, to resolve these problems, which has been approved by VINCE Labs.

Vulnerability Scoring Details

Item	CVE ID	CWE	CVSS v3.1 Base Score	CVSS v3.1 Vector
1	CVE-2025-13373	Improper Neutralization of Special Elements used in an SQL Command (CWE-89)	7.5	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

Vulnerability Type, Impact and Solution

Item	Vulnerability Type	Impact	Solution
1	Improper Neutralization of Special Elements used in an SQL Command (CWE-89)	The vulnerability can be exploited by unauthenticated users execute SQL command due to improperly restricted SNMPv1 trap validation.	Enhanced validate and sanitize all user inputs to ensure they conform to expected formats and do not contain any potentially harmful characters.

Affected Products

We strongly recommend all users update to the latest iView version as soon as possible. The update is available for download on our official website

Name	Vulnerabilities Fixed Version	Download Page
iView	5.8.01_7109	https://www.advantech.com/zh-tw/support/details/firmware?id=1-HIPU-183

Credits

Advantech would like to thank m00nback for disclosing the vulnerabilty and CISA for their collaboration on the coordinated disclosure process.

ADVANTECH Enabling an Intelligent Planet

No. 1, Alley 20, Lane 26, Rueiguang Road,
Neihu District, Taipei 11491, Taiwan, R.O.C.
Tel: 886-2-2792-7818
Fax: 886-2-2218-3650

Revision History

Version	Description	Release Date
1.0	First Advisory published	Nov. 24, 2025