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 WISE-6610

This document summarizes command injection vulnerabilities identified in the Advantech WISE-6610 industrial gateway, the associated CVEs, and the remediation actions completed by Advantech.

Vulnerability Type, Impact and Solution

Item	CVE ID	Impact	Solution
1	CVE-2026-2670	A command injection vulnerability exists in the OpenVPN file-deletion handling. User-controlled request data was concatenated into a shell rm command. Successful exploitation by a user with access to the affected management function could cause unintended operating-system commands to be executed on the gateway, potentially compromising device configuration and system integrity or availability.	The delete operation has been redesigned to map the requested file type to a fixed allowlisted path, require a numeric tunnel ID, reject invalid requests, and use the native filesystem API (fs.unlink) instead of constructing a shell command from request data.
2	CVE-2026-79697	A command injection vulnerability exists in the Basic Station certificate-deletion handling. The delete_file request value was directly concatenated into an os.execute("rm ...") command. Successful exploitation by a user with access to the affected management function could allow command injection or path manipulation, potentially resulting in arbitrary command execution or unauthorized file deletion.	The request is now mapped to one of the fixed internal certificate paths (trust, crt, or key). Invalid selectors are rejected with an HTTP 400 response, and the selected file is removed using fs.unlink rather than a shell command.
3	CVE-2026-79698	A command injection vulnerability exists in the Node-RED module-deletion handling. A client-supplied module name was used to construct an rm -r shell command without sufficient validation. Successful exploitation by a user with access to the affected management function could allow command injection or path manipulation, potentially altering files or executing unintended commands on the gateway.	Module names are trimmed and validated against a strict allowlist, path separators and invalid names are rejected, and the requested name must match an actual installed module before deletion. Raw request data is therefore no longer directly concatenated into the deletion command.

Credits

Advantech would like to thank the following researchers for responsibly reporting the vulnerabilities:

- CVE-2026-2670: jiefengliang (VulDB user)
- CVE-2026-79697, CVE-2026-79698: hubdk01 (VulDB user)

Additionally, Advantech would like to thank VulDB for its collaboration on the coordinated disclosure and CVE assignment process.

Affected Products

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

We strongly recommend all users update their devices to this latest firmware version as soon as possible. The update is available for download on our official website

Model Name	Download Page
WISE-6610-NB WISE-6610-EB WISE-6610-TB WISE-6610-JB WISE-6610-CB WISE-6610-EL-NB WISE-6610-EL-EB WISE-6610-EL-TB WISE-6610-EL-JB WISE-6610-EL-CB WISE-6610P-DEA WISE-6610P-DNA WISE-6610P-DTA	https://www.advantech.com/en-us/support/details/firmware?id=1-2K7AXRI

Revision History

Version	Description	Release Date
1.0	Initial WISE-6610 security advisory	Sep. 2, 2026