

SECURITY ADVISORY

Vulnerabilities Identified in ADAM-3600

This document summarizes the vulnerabilities identified in the ADAM-3600 product, the associated CVEs, and the remediation actions completed by Advantech.

Vulnerability Type, Impact and Solution

Item	CVE ID	NN ID	CVSS score	Impact	Solution
1	CVE-2026-43829	NN-2025-0091	9.2	when SafeEnhancement feature is enabled it is possible to send a base64 encoded password, however the size is not bounded and it allows an attacker to overflow the stack possibly leading to code execution.	Validate memory space size and avoid unsafe string or memory operations.
2	CVE-2026-43830	NN-2025-0092	8.6	When uploading a tampered firmware upgrade file during the verification of the file it is possible to inject commands.	Replace the md5sum command with OpenSSL's md5 function.
3	CVE-2026-43831	NN-2025-0122	9.2	An unauthenticated attacker could use the method for adding log message to overflow a stack buffer and possibly achieve code execution.	Validate memory space size and avoid unsafe string or memory operations.
4	CVE-2026-43832	NN-2025-0123	9.2	When the "SafeEnhancement" feature is enabled, an unauthenticated attacker could exploit a stack based buffer overflow to achieve code execution in the Cookie parsing methods.	Validate memory space size and avoid unsafe string or memory operations.
5	CVE-2026-43833	NN-2025-0124	7.5	An authenticated attacker could abuse the upload functionality to exploit a stack based buffer overflow, achieving code execution.	Validate memory space size and avoid unsafe string or memory operations.
6	CVE-2026-43834	NN-2025-0125	7.5	An authenticated attacker could abuse the logs settings functionality to exploit a stack based buffer overflow, achieving code execution.	Validate memory space size and avoid unsafe string or memory operations.
7	CVE-2026-43835	NN-2025-0126	8.6	An authenticated attacker could upload a forged firmware upgrade file possibly permanently compromising the device.	Asymmetric digital signature schemes.
8	CVE-2026-43836	NN-2025-0132	9.3	An attacker could forge a packet to execute arbitrary commands with maximum privileges.	Add content length validation for copied data. Add IP address format validation. Replace the system command with <code>execv + fork</code> .
9	CVE-2026-43837	NN-2025-0133	7.5	An attacker could exploit a buffer overflow with guest authentication in the password verify functionality to achieve code execution.	Validate memory space size and avoid unsafe string or memory operations.
10	CVE-2026-43838	NN-2025-0134	9.2	An attacker could exploit an issue in the log in functionality to overflow the	Validate memory space size and avoid unsafe

				stack leading to code execution.	string or memory operations.
11	CVE-2026-43839	NN-2025-0135	8.7	An unauthenticated attacker could exploit a NULL pointer dereference flaw in the logs management functionality to crash the service.	Add a null pointer check.
12	CVE-2026-43840	NN-2026-0001	6.9	An unauthenticated attacker could exploit a NULL pointer dereference flaw in the license manager service to make it crash. When the connection times out, the on_disconnected callback function is erroneously invoked twice . On the second invocation, the pointer to the connection string representation is NULL. This NULL pointer is passed to the apal_hash_remove_ex function wrapper, which internally calls strlen() on the pointer before any validation. This results in a memory access violation and crashes the service.	Added a null pointer check to the apal_hash_remove function in libAPAL to prevent errors. In libAPAL's apal_rpc module, added a connection status check before invoking the on_disconnected callback to avoid duplicate calls. In ElicMgr, added a check for whether cli->name is null within the on_disconnected callback function to prevent errors when calling apal_hash_remove.
13	CVE-2026-43841	NN-2026-0002	6.9	An unauthenticated attacker could exploit a NULL pointer dereference flaw in the license manager service to make it crash. Specifically, in the rpc_rx_fsm function, when rsp_flag_or_code is set to 0 while the msg_id remains valid, the response message structure is not initialized (remains NULL). However, subsequent message handlers still attempt to use this NULL pointer to build a response, causing a memory access violation and crashing the service.	The problems reflected in these two documents (NN-2026-0002 & NN-2026-0003) are essentially the same and can be resolved together. In the rpc_rx_fsm of libAPAL and apal_rpc, the original logic of determining whether to create a response packet based on the reply flag has been modified to always create a response packet. This ensures that a valid response packet pointer is always passed when invoking the message processing callback function, preventing potential abnormal access errors caused by the lack of pointer checking in the callback. After the callback function returns, the reply flag is then used to decide whether to discard the response packet or send its contents back to the communicating party.

14	CVE-2026-43842	NN-2026-0003	6.9	An unauthenticated attacker could exploit a NULL pointer dereference flaw in the license manager service to make it crash. The issue resides in the <code>rpc_rx_fsm</code> function. When <code>msglen</code> is set to 0 but the <code>msg_id</code> corresponds to a handler that expects an inner message payload, the service crashes upon the first call to <code>apal_rpc_msg_read_element</code> or <code>apal_rpc_msg_get_element_ptr</code> . The crash occurs because no validation is performed on the message structure pointer before it is used.	The problems reflected in these two documents (NN-2026-0002 & NN-2026-0003) are essentially the same and can be resolved together. In the <code>rpc_rx_fsm</code> of <code>libAPAL</code> and <code>apal_rpc</code> , the original logic of determining whether to create a response packet based on the reply flag has been modified to always create a response packet. This ensures that a valid response packet pointer is always passed when invoking the message processing callback function, preventing potential abnormal access errors caused by the lack of pointer checking in the callback. After the callback function returns, the reply flag is then used to decide whether to discard the response packet or send its contents back to the communicating party.
15	CVE-2026-43843	NN-2026-0004	6.9	An unauthenticated attacker could exploit an integer overflow error in the license manager service to make it crash.	In the <code>rpc_rx_fsm</code> of <code>libAPAL</code> and <code>apal_rpc</code> , a maximum value check is added for the length of received packets, i.e., <code>data_len < UINT32_MAX</code> , to prevent arithmetic overflow caused by all 0xFF values.
16	CVE-2026-43844	NN-2026-0005	9.3	An attacker could bypass the authentication mechanism on the proprietary protocol.	Remove the singleton pattern to prevent command conflicts between port 6001 and port 7001. Currently, different commands are implemented on port 7001 and port 6001.
17	CVE-2026-43845	NN-2026-0006	9.2	An attacker could bypass the authentication mechanism by carefully exploiting the password reset mechanism.	The password recovery function has been modified to only perform recovery when the status is checked during the first power-on. If the program restarts after an exception caused by an attack, the password

					will not be reset to the default.
18	CVE-2026-43846	NN-2026-0007	8.6	An authenticated attacker could exploit a non functional feature to overflow the stack leading to code execution.	Delete command 164.
19	CVE-2026-43847	NN-2026-0008	8.2	An attacker could bruteforce the administrator password on the proprietary protocol without restrictions, even when SafeEnhancement feature is enabled.	Add a lockout function after password verification failures. After 5 consecutive failed connection attempts, a 5-minute waiting period is required before verification can continue.
20	CVE-2026-43848	NN-2026-0009	6.9	An unauthenticated attacker could abuse the functionality of bulk setting the device ports to crash the service.	Delete command 173.
21	CVE-2026-43849	NN-2026-0010	6.9	An attacker could exploit a functionality to read past the heap allocated memory leaking potentially sensitive data.	Add bounds checking.
22	CVE-2026-43850	NN-2026-0011	8.6	An authenticated attacker could exploit a command injection vulnerability to achieve root code execution on the system.	Disable the script execution capability of AdvProgramMgr, and disallow commands starting with /bin/sh. Restrict project download access exclusively to the /home/sysuser/project directory. Prohibit AdvProgramMgr from executing any programs located under the /home/sysuser/project directory. The above controls can effectively prevent privilege escalation operations induced by malicious scripts or program file downloads.
23	CVE-2026-43851	NN-2026-0012	8.2	An authenticated attacker could exploit a functionality to read arbitrary files on the system. The vulnerability exists in the CommandFileDownload::Execute function of the mod_projectmr library, specifically in the handler for message ID 104 (Upload Start). The CommandFileDownload::GetFileName function concatenates a destination directory (selected based on an integer value in the payload) with a user-supplied path. No validation is performed on the user-supplied path, allowing an attacker to use relative path sequences (e.g., ../../) to escape	Starting from version 2.8.5.1, the system will be available in a Standard Edition and an SE Security Enhanced Edition. • For the Standard Edition, the read/write directories are /tmp/ and /home/sysuser. • For the SE Security Enhanced Edition, the read/write directories are /tmp, /home/sysuser/project, and /home/www/xml.

				the intended project directory and read any file on the system.	
24	CVE-2026-43852	NN-2026-0013	8.2	An authenticated attacker could exploit a functionality to write arbitrary files on the system. The vulnerability exists in the CommandFileDownload::Execute function of the mod_projectmr library, specifically in the handler for message ID 101 (Download Start). The function concatenates a destination directory (selected based on an integer value in the payload) with a user-supplied path. No validation is performed on the user-supplied path, allowing an attacker to use relative path sequences (e.g., ../../) to escape the intended project directory and write files to arbitrary locations on the system.	Starting from version 2.8.5.1, the system will be available in a Standard Edition and an SE Security Enhanced Edition. • For the Standard Edition, the read/write directories are /tmp/ and /home/sysuser. • For the SE Security Enhanced Edition, the read/write directories are /tmp, /home/sysuser/project, and /home/www/xml.
25	CVE-2026-43853	NN-2026-0014	8.2	An attacker could send a message to trigger an assertion that causes the service to be closed.	In the CBufferPool::IsValid function, assertions are no longer used to handle the condition m_nBufferSize < MAX_BUFFER_SIZE. Instead, this constraint is enforced during the assignment of m_nBufferSize to ensure m_nBufferSize is always less than MAX_BUFFER_SIZE.
26	CVE-2026-43854	NN-2026-0015	6.3	An attacker having access to the encrypted project file could retrieve the credentials for administrator access of EdgeLink enabled devices.	Compress project files using password-protected ZIP with AES-256 encryption. Use a high-strength password as the default password. Provide an interface for users to set passwords for project files. When opening a project, if it is detected that the project does not use the default password, a pop-up window will prompt the user to enter the password. If an older version project is detected, the user will be prompted to apply the default password. Users can modify the password on the project configuration page.
27	CVE-2026-43855	NN-2026-0016	7.5	This vulnerability allows a remote authenticated attacker to execute arbitrary code, the issue results from the lack of proper validation of the length of user input prior to copying it	Add checks for file names and their lengths.

				to a heap based buffer.	
28	CVE-2026-43856	NN-2026-0017	8.6	This vulnerability allows a remote authenticated attacker to execute arbitrary code, the issue results from the lack of proper validation of the length of user input prior to copying it to a stack based buffer. The vulnerability exists in the FileProcess::CheckDir function, which is called from the FileProcess constructor when handling a Download Start message (message ID 101) on port 6001. The CheckDir function copies a user-supplied path into a local stack buffer of only 1024 bytes using strcpy, without any length validation. Although the overall path length may be limited to PATH_MAX (4096 bytes) elsewhere in the code, the CheckDir function does not enforce this limit. An attacker can provide a path longer than 1024 bytes, overflowing the stack buffer and overwriting saved registers and the return address, leading to arbitrary code execution.	Add a check for the filename length. Modify and unify the buffer length related to filenames and paths to 4096. Restrict the file download location. Replace the original mkdir command with calling the mkdir() function to create the relevant missing directories.
29	CVE-2026-43857	NN-2026-0018	8.6	This vulnerability allows a remote authenticated attacker to execute arbitrary code, the issue results from the lack of proper validation of the length of user input prior to copying it to a stack based buffer. The vulnerability exists in the FileProcess::CheckDir function when handling a Download Start message (message ID 101) on port 6001. If the specified directory path does not exist, the function constructs a shell command using sprintf to create a mkdir -p command string, then executes it via the system() function. The user-supplied path is directly embedded into the command string without any validation or sanitization. An attacker can provide a crafted path containing shell metacharacters (e.g., backticks, semicolons, or command substitutions), which will be executed by system() with the privileges of the service.	Add a check for the filename length. Modify and unify the buffer length related to filenames and paths to 4096. Restrict the file download location. Replace the original mkdir command with calling the mkdir() function to create the relevant missing directories.
30	CVE-2026-43858	NN-2026-0019	8.6	An authenticated remote attacker could abuse a functionality to exploit a stack based buffer overflow leading to arbitrary code execution.	Add user input length validation.

Credits

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

- Simone Bossi and Raffaele Bova at Nozomi Networks.

Additionally, Advantech would like to thank CSA for their collaboration on the coordinated disclosure process.

Affected Products

We strongly recommend all users update their devices to this latest firmware version (EdgeLink v2.8.5.0) as soon as possible. The update is available for download on our official website.

In the latest firmware version (EdgeLink v2.8.5.0), ADAM-3600 has fixed all the above vulnerabilities.

Model Name	Download Page
ADAM-3600	ADAM-3600-C2G EdgeLink Image - 研华技术支持

Revision History

Version	Description	Release Date
1.0	First Advisory published	October,12,2026