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 EKI-1242EIMS/EKI-1242IEIMS

A security update is now available to address several security vulnerabilities identified in previous firmware versions of the EKI-1242EIMS and EKI-1242IEIMS, including OS command injection, code injection, unauthorized access, signature verification, encrypted communication protection, and Cross-Site Request Forgery (CSRF)-related vulnerabilities.

Firmware version 2.00.01 has been officially released to address these security vulnerabilities and enhance the overall security of the devices. Users are strongly encouraged to update their devices to the latest firmware version available on the official website to ensure optimal security protection.

Vulnerability Scoring Details

Item	CVE ID	CWE	CVSS v4.0 Base Score	CVSS v4.0 Vector
1	CVE-2026-73177	CWE-345 Insufficient Verification of Data Authenticity	**8.6**	CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
2	CVE-2026-73176	CWE-78 OS Command Injection	**8.6**	CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
3	CVE-2026-73175	CWE-400 Uncontrolled Resource Consumption	**7.1**	CVSS:4.0/AV:A/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N
4	CVE-2026-73174	CWE-319 Cleartext Transmission of Sensitive Information	**8.7**	CVSS:4.0/AV:A/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
5	CVE-2026-73173	CWE-306 Missing Authentication for Critical Function	**8.8**	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:H/VA:H/SC:N/SI:N/SA:N
6	CVE-2026-73172	CWE-78 OS Command Injection	**9.3**	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
7	CVE-2026-73171	CWE-73 External Control of File Name or Path	**8.6**	CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
8	CVE-2026-73170	CWE-94 Code Injection	**8.6**	CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
9	CVE-2026-73169	CWE-79 Cross-site Scripting (Stored XSS)	**6.3**	CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:P/VC:L/VI:L/VA:N/SC:H/SI:H/SA:H
10	CVE-2026-73168	CWE-78 OS Command Injection	**8.6**	CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
11	CVE-2026-73167	CWE-78 OS Command Injection	**8.6**	CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N

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

Item	CVE ID	CWE	CVSS v4.0 Base Score	CVSS v4.0 Vector
12	CVE-2026-73166	CWE-94 Code Injection	**8.6**	CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
13	CVE-2026-73165	CWE-78 OS Command Injection	**8.6**	CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
14	CVE-2026-73164	CWE-78 OS Command Injection	**8.6**	CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
15	CVE-2026-73163	CWE-78 OS Command Injection	**8.6**	CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
16	CVE-2026-19535	CWE-352 Cross-Site Request Forgery (CSRF)	**8.6**	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N

Vulnerability Type, Impact and Solution

Item	Vulnerability Type	Impact	Solution
1	Insufficient Verification of Data Authenticity — firmware upgrade lacks signature verification	An administrator-level attacker can upload and flash arbitrary unsigned firmware, gaining full and persistent control of the platform.	Introduce cryptographic firmware image signing and mandatorily verify the signature against a trusted public key embedded in the device; unconditionally reject any image without a valid signature, and require signed vendor metadata as part of the upgrade acceptance criteria.
2	OS Command Injection — OPC UA security settings page, remove_file parameter	An authenticated remote attacker can inject arbitrary shell commands via the remove_file parameter and execute them as root, achieving remote code execution on the device.	Whitelist remove_file (allow only root_ca / key_pair); replace shell-backed grep/echo with nixio.fs or the UCI Lua API; change the route to post() to enforce POST; use luci.util.shellquote() where shell calls are unavoidable.
3	Uncontrolled Resource Consumption — OPC UA session-pool exhaustion	An adjacent unauthenticated attacker can open many anonymous sessions; heap exhaustion (BadOutOfMemory) occurs at ~40 sessions and denies service to all legitimate OPC UA clients (DoS).	The configured OPC UA session limit is reduced from 128 to 32 to prevent memory exhaustion. Users are also advised to disable anonymous access to reduce the risk of denial-of-service (DoS) attacks.
4	Cleartext Transmission of Sensitive Information — edgserver management protocol (TCP/UDP 5058)	A passive observer on the network path can intercept cleartext management traffic and recover device identity and network metadata (model, name, MAC, IP, netmask, gateway); a suitably positioned attacker can also mount a MitM attack to modify traffic.	After production testing, perform a factory-default reset so that the test-only edgserver component is disabled before shipment. For devices already shipped with an earlier version, install this update and perform a one-time reset to the default configuration; doing so disables edgserver and eliminates exposure to this vulnerability.
5	Missing Authentication for Critical Function — edgserver management protocol (TCP 5058)	An unauthenticated remote attacker can directly invoke critical management functions including network reconfiguration, reboot, factory reset, firmware upgrade and auxiliary-channel setup; the protocol relies only on weak targeting fields (magic/version/model/MAC) rather than authentication.	After production testing, perform a factory-default reset so that the test-only edgserver component is disabled before shipment. For devices already shipped with an earlier version, install this update and perform a one-time reset to the default configuration; doing so disables edgserver and eliminates exposure to this vulnerability.
6	OS Command Injection — edgserver monitor handler (unauthenticated)	An unauthenticated remote attacker can send a crafted monitor request to TCP 5058; the controlled string is formatted via sprintf into a command and executed by system() as root,	Validate the MAC input to prevent injection attacks. After production testing, perform a factory-default reset so that the test-only edgserver component is disabled before shipment. For devices already shipped with

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

Item	Vulnerability Type	Impact	Solution
		achieving arbitrary command execution and full device compromise.	an earlier version, install this update and perform a one-time reset to the default configuration; doing so disables edgserver and eliminates exposure to this vulnerability.
7	External Control of File Name or Path — backup / restore workflow	An authenticated remote attacker can upload a crafted backup archive that, after only a weak model-pattern check, is extracted to the root filesystem as root, overwriting arbitrary files (e.g. startup scripts) to gain persistent code execution.	Do not extract restore archives to / based only on a model-pattern check; restrict restore to an explicit allowlist of expected config files and directories, reject unexpected archive members, validate paths before extraction, and add cryptographic authenticity checks for restore archives.
8	Code Injection — Modbus CSV import generates Lua source	An authenticated remote attacker can place crafted content in the imported transaction-name field, break out of the Lua string literal generated by csv_parser, and execute attacker-controlled Lua code during CSV import.	Do not generate executable Lua source from imported CSV fields; use direct structured configuration updates, or apply strict context-appropriate escaping before inserting any controlled value; enforce strict server-side validation of imported transaction names.
9	Stored Cross-site Scripting — Modbus transaction management interface	An authenticated remote attacker can store malicious script in metadata fields such as the transaction name; it executes in an administrator's browser context when they later open an affected management page (transaction list, Data View, Mapping, etc.).	Apply context-appropriate output encoding to all controlled values before rendering into LuCI templates or JSON-backed tables; replace raw <%= rendering with pcdata(...) or an equivalent escaping helper; review other templates for the same unsafe pattern.
10	OS Command Injection — download_gsdml_apply, subcategory parameter	An authenticated remote attacker can inject shell syntax via the subcategory parameter and execute arbitrary commands as root (confirmed via a timing/sleep payload).	Do not interpolate user input into shell command strings; use an argument-safe execution method and constrain subcategory to a strict allowlist of expected protocol identifiers.
11	OS Command Injection — remote_server_apply, log_hostname parameter	An authenticated remote attacker can inject shell syntax via syslog-configuration parameters (log_hostname, etc.) and execute arbitrary commands as root.	Replace shell-backed configuration updates with direct API calls, validate syslog-related parameters against strict expected formats, and never concatenate any request parameter into a shell command.
12	Code Injection — python_scrip_apply executes arbitrary Python	An authenticated remote attacker can submit arbitrary Python source that the device runs as root (os.popen('id') returned uid=0(root)), reaching operating-system command execution in a privileged context.	Remove direct execution of user-supplied Python from the web interface; if script automation is required, enforce strong access-control boundaries, isolate the execution environment, apply explicit allowlists, and prevent the feature from invoking unrestricted OS primitives.
13	OS Command Injection — python_manager_apply, package parameter (uninstall)	An authenticated remote attacker can inject shell syntax via the package parameter when act=uninstall, executing arbitrary commands as root.	Do not invoke package-management commands through shell string concatenation; use an argument-safe execution primitive or a higher-level package-management API, and restrict uninstall targets to validated package identifiers.
14	OS Command Injection — pnlog_level_apply, pnlog_level parameter	An authenticated remote attacker can inject shell syntax via the pnlog_level parameter and execute arbitrary commands as root.	Replace shell-based writes with safe file or configuration APIs; enforce a strict server-side allowlist of accepted log-level values and avoid passing request data through a shell interpreter.
15	OS Command Injection — opcua_set_apply, hostname parameter	An authenticated remote attacker can inject shell metacharacters via the hostname parameter and achieve command execution as root.	Avoid building shell commands from request parameters; perform UCI operations through a direct configuration API and validate hostname server-side against a strict allowlist of expected characters.

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

Item	Vulnerability Type	Impact	Solution
16	Cross-Site Request Forgery (CSRF) — LuCI administrative interface	An unauthenticated remote attacker can cause a logged-in administrator's browser to submit forged state-changing requests, abusing privileged functions across the management interface, including high-impact configuration changes and the web-exposed Python execution capability.	Require anti-CSRF validation (per-request CSRF token or equivalent POST-security check) for all state-changing vendor administrative actions; add extra confirmation or re-authentication to especially sensitive operations such as reset, restore, firmware management and script execution.

Affected Products

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	Vulnerabilities Fixed Version	Download Page
EKI-1242EIMS EKI-1242IEIMS	V2.00.01	https://www.advantech.com/en/support/details/firmware-?id=1-1JQK6HR

Acknowledgement

These vulnerabilities have been discovered by Simone Bossi from Nozomi Networks Labs.

Revision History

Version	Description	Release Date
1.0	First Advisory published	Sep. 4, 2026