Document: CYB/2026/86278/Advisory
Revision: 1.0
Date: 20-JULY-2026

CYBERSECURITY VULNERABILITY ADVISORY

Two Vulnerabilities in ASE2000 V2 Communication Test Set - Improper Certificate Validation (IEC 60870-5-104 TLS Client) and Bundled Third-Party Library (Apache log4net XXE)

ASE/Kalkitech Vulnerability ID: CYB/2026/86278

External Vulnerability ID(s)

CVE ID (Apache log4net): CVE-2018-1285

CVE ID (IEC 60870-5-104 TLS client): CVE-2026-xxxxx [to be filed with CVE and updated with new CVE number]

SUMMARY

Two security vulnerabilities have been identified affecting the ASE2000 V2 Communication Test Set.

The first vulnerability is present in a third-party logging library, Apache log4net version 2.0.8.0, which is bundled with the product. The XML configuration parser used by this library does not disable XML external entity (XXE) processing (CVE-2018-1285). An attacker able to supply or modify the application's log4net configuration file on the host could read or write arbitrary local files, or cause the application to issue outbound network requests (Server-Side Request Forgery). Exploitation requires access to the configuration file on the host; file access is limited to the privilege of the user executing the application.

The second vulnerability is present in the IEC 60870-5-104 TLS client (Task Mode). The server-certificate validation logic does not correctly reject certificates when multiple certificate errors occur simultaneously; certain combinations of certificate faults are accepted instead of rejected. As a result, a self-signed or otherwise invalid certificate presented with a mismatched host name can pass validation. A network-positioned attacker able to intercept the connection can impersonate the trusted peer, complete the TLS handshake, and read or modify the protected communications (Man-in-the-Middle).

ASE/Kalkitech provides an upgraded version (2.38) that resolves both vulnerabilities. The Apache log4net vulnerability affects all released versions from 2.25 up to and including 2.37. The IEC 60870-5-104 TLS certificate validation vulnerability affects all released versions from 2.35 up to and including 2.37.

SEVERITY

The vulnerabilities have been assessed using the Common Vulnerability Scoring System (CVSS) and have the following characteristics.

Vulnerability 1 – Apache log4net XML External Entity (CVE-2018-1285)
CWE: CWE-611 (Improper Restriction of XML External Entity Reference)

CVSS v3.1 Base Score: 9.8 (Critical)
CVSS v3.1 Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
Impact Subscore: 5.9
Exploitability Subscore: 3.9
CVSS Temporal Score: NA
CVSS Environmental Score: NA
Modified Impact Subscore: NA
Overall CVSS Score: 9.8

The score above is the published NVD base score for CVE-2018-1285. In the context of the ASE2000 deployment, the log4net configuration file is local to the host and is not exposed over the network; practical exploitation therefore requires local or file-system access to the host. The Environmental Impact score has not been calculated since it depends on the deployment environment. Affected users are recommended to compute the environmental score according to the characteristics of their deployment.

CVSS v3.1 Calculation NVD Link:
https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?name=CVE-2018-1285&vector=AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H&version=3.1&source=NIST

Vulnerability 2 – IEC 60870-5-104 TLS Client Improper Certificate Validation
CWE: CWE-295 (Improper Certificate Validation)

CVSS v3.1 Base Score: 7.4 (High)
CVSS v3.1 Vector: AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N
Impact Subscore: 5.2
Exploitability Subscore: 2.2
CVSS Temporal Score: NA
CVSS Environmental Score: NA
Modified Impact Subscore: NA
Overall CVSS Score: 7.4

CVSS v4.0 Base Score: 9.1 (Critical)
CVSS v4.0 Vector: AV:N/AC:H/AT:N/PR:N/UI:N/VC:H/VI:H/VA:N/SC:N/SI:N/SA:N

Exploitation requires the attacker to occupy a man-in-the-middle position on the network path between the ASE2000 client and its intended TLS peer. The Environmental Impact score has not been calculated since it depends on the deployment environment. Affected users are recommended to compute the environmental score according to the characteristics of their deployment.

CVSS v3.1 Calculation NVD Link:
https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N

CVSS v4.0 Calculation NVD Link:
https://nvd.nist.gov/vuln-metrics/cvss/v4-calculator?vector=AV:N/AC:H/AT:N/PR:N/UI:N/VC:H/VI:H/VA:N/SC:N/SI:N/SA:N

VULNERABILITY DETAILS

Vulnerability 1 – Apache log4net XML External Entity (CVE-2018-1285)

The ASE2000 V2 Communication Test Set bundles Apache log4net version 2.0.8.0 (log4net.dll), which is statically referenced by the main application and initialized at application start-up. Versions of log4net prior to 2.0.10 do not disable XML external entity processing when parsing the log4net configuration file. An attacker who can control or alter that configuration file can use external-entity references to read local files, write files, or trigger outbound network connections from the host (SSRF). The file access is limited to the privilege of the user executing the application.

Vulnerability 2 – IEC 60870-5-104 TLS Client Improper Certificate Validation

When the ASE2000 IEC 60870-5-104 client (Task Mode) establishes an outbound TLS connection, the server certificate is evaluated by a validation routine. The routine handles individual certificate-error conditions correctly but does not reject certain combinations of simultaneous certificate errors; these combined conditions are accepted as valid. The most readily triggered case is a self-signed certificate presented with a host name that does not match the expected peer, which produces both a name-mismatch and a chain/trust error at the same time and is incorrectly accepted. An attacker positioned between the client and its intended peer can present such a certificate, complete the TLS handshake, and subsequently read and modify the traffic exchanged over the connection. This undermines the confidentiality and integrity

that TLS is intended to provide for IEC 60870-5-104 communications. Exploitation requires network access and a man-in-the-middle position between the client and its peer.

AFFECTED PRODUCTS

Product: ASE2000 V2 Communication Test Set.

- Apache log4net vulnerability (CVE-2018-1285): All released versions from 2.25 (released on 19-Oct-2020) up to and including 2.37 (released on 29-May-2026).
- IEC 60870-5-104 TLS client certificate validation vulnerability: all released versions from 2.35 (released on 8-Apr-2025) up to and including 2.37 (released on 29-May-2026).

MITIGATION OR RESOLUTION

ASE/Kalkitech provides an upgraded version 2.38 that fixes both vulnerabilities. Customers are advised to upgrade to version 2.38. In version 2.38 the bundled log4net library is upgraded to version 3.3.1.0, and the IEC 60870-5-104 TLS client certificate validation logic is corrected to ensure proper validation of certificate error conditions.

All customers running ASE2000 versions 2.25 through 2.37 are affected by this issue and are required to upgrade to version 2.38 or later to apply the security fix. Upgrade instructions and user documentation are available at www.ase-systems.com. For detailed, step-by-step guidance on upgrading to the latest version and patching the impacted components, please contact our support team at support@ase-systems.com.

Until the upgrade can be applied, the following interim measures reduce exposure:

- Restrict write access to the ASE2000 installation directory and its configuration files to trusted administrators only.
- Avoid using IEC 60870-5-104 over TLS across untrusted or shared networks; place ASE2000 hosts on an isolated, segmented network reachable only by intended peers.
- Ensure the host is protected by a network firewall.

STATUS OF THE VULNERABILITY

These vulnerabilities were reported to ASE/Kalkitech through responsible disclosure and were also reported by the researcher to the United States Cybersecurity and Infrastructure Security Agency (CISA). As of the time of this writing, ASE/Kalkitech has not received any information indicating that these vulnerabilities have been exploited in customer environments.

The Apache log4net vulnerability is publicly tracked as CVE-2018-1285. A CVE identifier for the IEC 60870-5-104 TLS client certificate validation issue is being coordinated through CISA / ICS-CERT and will be added to this advisory when assigned. This advisory will be revised at that time to reflect the assigned identifier.

CREDITS AND ACKNOWLEDGEMENTS

ASE/Kalkitech gratefully acknowledges the following persons/organizations for their support.

- Mr. Enoch Wang (enochsurge@gmail.com) – for detecting and reporting the vulnerabilities and providing proof-of-concept code, coordinated through CISA.