CYBERSECURITY VULNERABILITY ADVISORY

Vulnerability in ASE61850 IEDSmart – Remote Code Execution and Arbitrary File Read

Kalkitech/ASE Vulnerability ID: CYB/2024/60704

External Vulnerability ID(s)

CVE ID: CVE-2024-36059

DISCLAIMER

The information in this document is subject to change without notice and should not be construed as a commitment by Kalkitech / ASE.

Kalkitech/ASE provide no warranty, express or implied, including warranties of merchantability and fitness for a particular purpose, for the information contained in this document, and assumes no responsibility for any errors that may appear in this document. In no event shall Kalkitech, ASE or any of their suppliers be liable for direct, indirect, special, incidental or consequential damages of any nature or kind arising from the use of this document, or from the use of any hardware or software described in this document, even if Kalkitech/ASE have been advised of the possibility of such damages.

This document and parts hereof must not be reproduced or copied without written permission from Kalkitech/ASE and the contents hereof must not be provided to a third party nor used for any unauthorized purpose.

SUMMARY

A security vulnerability reported in the ASE61850 IEDSmart product, allows an attacker to read arbitrary files in and write files back to the host Computer. The attack requires network access to the Computer and knowledge of its IP address, as well as knowledge of IEC61850 File Transfer protocols and its implementation. The attack exploits the lack of Path Traversal control in the product when performing File Reads/Writes using the IEC61850 Protocol, thus allowing RCE (Remote Code Execution) and Arbitrary File read in the host Computer. The file access is limited to the privilege of the user executing the application

Kalkitech/ASE provides an upgraded version that secures the File Transfer operation and eliminates this vulnerability. This vulnerability affects all release versions upto and including version 2.3.5 of the product

SEVERITY

The vulnerability has been assessed using the Common Vulnerability Scoring System v2 and has the following characteristics

CVSS Base Score: 9.0

Impact Subscore: 9.5

Exploitability Subscore: 8.6

CVSS Temporal Score: 7.4

CVSS Environmental Score: NA

Modified Impact Subscore: NA

Overall CVSS Score: 7.4

CVSS V2 Vector: (AV:N/AC:M/Au:N/C:C/I:P/A:C/E:F/RL:OF/RC:C)

The Environmental Impact score has not been calculated since it depends on the deployment environment. Affected users are recommended to compute the environmental impact according to the characteristics of their deployment.

CVSSv2 Calculation NVD Link:

https://nvd.nist.gov/vuln-metrics/cvss/v2-calculator?vector=(AV:N/AC:M/Au:N/C:C/I:P/A:C/E:F/RL:OF/RC:C)

VULNERABILITY DETAILS

The product simulates IEC61850 Server devices and supports the IEC61850 File Transfer service allowing Client applications to read/write files in the Simulated device’s FileStore. The product provides a FileStore location in the Computer’s disk. The vulnerability is caused due to not restricting/controlling the file path used by a client application to read and write files to the product. The exploit requires network access to the device and knowledge of its IP address as well as knowledge of IEC61850 Protocol and its implementation.

AFFECTED PRODUCTS

Products: ASE61850 IEDSmart, all released versions upto and including version 2.3.5.

MITIGATION OR RESOLUTION

Kalkitech/ASE provides an upgraded version that fixes this vulnerability. Customers are advised to uninstall version 2.3.5 and previous versions and install the provided upgrade

The patch as well as user instructions are distributed to validated customers through their Kalki.io accounts. Affected customers who have not activated their Kalki.io device-management account may contact support@kalkitech.com to receive the same.

STATUS OF THE VULNERABILITY

This vulnerability has been reported to Kalkitech/ASE through responsible disclosure and is not known to be in the public domain as of the time of this writing. Kalkitech/ASE has not received any information that this vulnerability has been exploited as of date.

As part of good/ethical practice in handling known vulnerabilities, this vulnerability will be submitted to CVE and/or other Security repository agencies in a reasonable duration of time from the date of this advisory. This advisory will be revised at that time with the CVE ID and to reflect the fact that the issue has been submitted in the public domain.

CREDITS AND ACKNOWLEDGEMENTS

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

- Mr. Alain Rödel (alain@neodyme.io), Neodyme AG

For detecting and reporting the vulnerability and providing proof of concept code.