Date: 16-AUGUST-2021

CYBERSECURITY VULNERABILITY ADVISORY
Vulnerability in SYNC product family – Unsecured Administration link
Kalkitech/ASE Vulnerability ID: CYB/2021/33631

External Vulnerability ID(s)

CVE ID: CVE-2021-44564

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.

All rights to registrations and trademarks reside with their respective owners.

SUMMARY

A security vulnerability originally reported in the SYNC2101 product, and applicable to specific subfamilies of SYNC devices, allows an attacker to download the configuration file used in the device and apply a modified configuration file back to the device. The attack requires network access to the SYNC device and knowledge of its IP address. The attack exploits the unsecured communication channel used between the administration tool Easyconnect and the SYNC device (in the affected family of SYNC products)

Kalkitech/ASE provides an upgrade patch that secures the administration channel and eliminates this vulnerability. Not all SYNC devices are vulnerable to this issue. Please see “AFFECTED PRODUCTS” sections to verify if your SYNC installations are susceptible and require the proposed mitigations to be applied

SEVERITY

The vulnerability has been assessed using the Common Vulnerability Scoring System v2 and has the following characteristics CVSS Base Score: 10.0

Impact Subscore: 10.0

Exploitability Subscore: 10.0

CVSS Temporal Score: 8.3

CVSS Environmental Score: NA

Modified Impact Subscore: NA

Overall CVSS Score: 8.3

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

VULNERABILITY DETAILS

The vulnerability is caused due to an unsecured communication channel used to configure the device. The exploit requires network access to the device and knowledge of its IP address.

AFFECTED PRODUCTS

Products: Following product variants running GPC version 4.15.3 and below are affected

SYNC200 – SYNC221 M1, SYNC241 M1/M2/M4, SYNC261-M1

SYNC2000 - SYNC2000-M1/M2/M4

SYNC2100 - SYNC2101-M1/M2/M6/M7/M8

SYNC2111 - SYNC2111-M2/M3

SYNC3000 – SYNC3000-M1/M2/M3/M4/M12– [Note: In this product range, Device Generation – "GEN_C" specifically is not susceptible to this issue]

NOTE: These products traditionally supported an option (offered to security-sensitive installations) called the CIP DCCP patch that served to secure the communication channel. However, this option is NO LONGER recommended due to new vulnerabilities detected in supporting libraries.

MITIGATION OR RESOLUTION

Kalkitech/ASE provides an upgrade patch that can be installed to the affected devices using the default Easyconnect utility. Application of this patch secures the administration channel and eliminates this vulnerability.

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.Imran Jamadar, Mr.Vedant Gavde, Mr.Shahrukh Khan, Mr.Faruk Kazi, and Mr.Sunil G Bhirud, -
From CoE CNDS VJTI, Mumbai, India. (imjamadar_p19@ce.vjti.ac.in)

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