CYBERSECURITY VULNERABILITY ADVISORY

Vulnerability in SYNC3000 Substation DCU – Webserver Command Injection

Kalkitech/ASE Vulnerability ID: CYB/2019/19561

External Vulnerability ID(s)

CVE ID: CVE-2019-11536

SUMMARY

A security vulnerability in the SYNC3000 product allows an attacker to inject client-side commands or scripts to be executed in the device with privileged access. The attack requires network connectivity to the device and exploits the webserver interface, typically through a browser

Kalkitech/ASE provides a patch that sanitizes the application and eliminates this vulnerability. Not all versions of SYNC3000 devices are vulnerable to this issue. Please see “AFFECTED PRODUCTS” sections to verify if your SYNC3000 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 insufficient sanitization of user entered fields submitted to the webserver.

AFFECTED PRODUCTS

Product: SYNC3000 Family of Substation DCU/Gateways

Versions: GPC v2.22.6, 2.23.0, 2.24.0, 3.0.0, 3.1.0, 3.1.16, 3.2.3, 3.2.6, 3.5.0, 3.6.0 and 3.6.1 releases where WebHMI module is NOT installed. Specifically, if WebHMI module is installed, these versions are NOT susceptible to this issue.

Also, specifically, v4.x releases onwards are NOT susceptible.

MITIGATION OR RESOLUTION

Kalkitech/ASE provides a patch executable that can be installed to the affected devices using the default Easyconnect utility. Application of this patch sanitizes the application 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.

Mathieu Bergeron-Legros – mbl@victrix.ca – Victrix

Samuel De Grace - sdegrace@vumetric.com – VuMetric

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