gemalto
a Thales company

# Security Bulletin

## Bulletin Number
20191107

## Issue Date
20191108

## Severity Level
Medium

## CVE

[CVE-2019-8281]
[CVE-2019-8284]

## Known Exploits
None

## Mitigation Provided
Yes

## Customer Support
For further questions or concerns, please contact Gemalto technical support at https://supportportal.gemalto.com/

# Vulnerabilities in Sentinel LDK Admin Control Center

## Description
The Sentinel LDK Admin Control Center is impacted by the following vulnerabilities:

-       A weakness in the Cross-Site Request Forgery (CSRF) protection mechanism could potentially allow unauthorized actions, such as configuration parameter changes in Sentinel LDK Admin Control Center.
-       Remote access only available over HTTP allowing man-in-the-middle attack to steal sensitive data.

## Products Affected
Sentinel LDK RTE versions lower than version v7.102.

## Mitigation
Customers who have Sentinel LDK Runtime version lower than version 7.102 are advised to upgrade to Sentinel LDK Runtime version 7.102 or later in order to enable this security update.

https://sentinelcustomer.gemalto.com/sentineldownloads/

*Gemalto acknowledges and thanks Artem Zinenko from Kaspersky Lab ICS CERT for responsible disclosure of these vulnerabilities.*