



# Security Bulletin

**Bulletin Number**

20190429

**Issue Date**

2019 May 01

**Severity Level**

Medium

**CVE**

[CVE-2019-8282]

[CVE-2019-8283]

**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:

- Use of clear text HTTP communication could potentially allow a man-in-the-middle attack by replacing the original language pack by malicious one; and
- Absence of an HTTPOnly attribute in LDK LMS (License Management Service) could allow unauthorized access to cookies by using malicious JavaScript.

**Products Affected**

Sentinel LDK RTE versions lower than version v7.92.

**Mitigation**

Customers who have Sentinel LDK Runtime version lower than version 7.92 are advised to upgrade to Sentinel LDK Runtime version 7.92 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.*