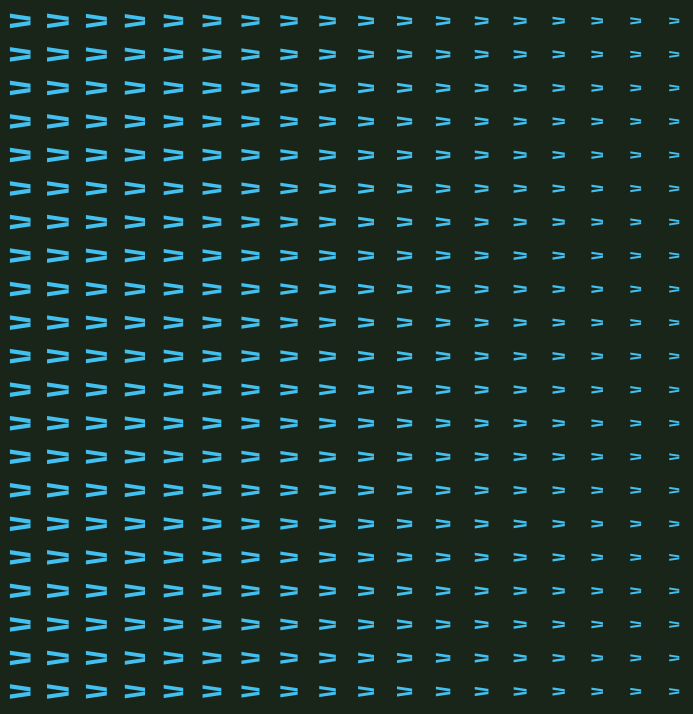
salto
INSPIRED ACCESS

Version 1.0 (Nov, 2026)

SECURITY ADVISORY

Salto Security Advisory Danalock (V3)



SALTO ECOSYSTEM

Confidential –Limited Distribution

Salto has released a security update for the Salto Danalock product mobile apps and SDK that addresses an issue affecting communication between the mobile application and the lock.

Under specific conditions, a nearby attacker could intercept authentication credentials exchanged between the mobile application and the Danalock device.

There is no indication of widespread exploitation, and the issue has been remediated through a software update.

Security Advisory

SALTO SECURITY ADVISORY
DANALOCK

Salto Product Security Advisory

Product: Danalock
Issue: Man in the middle attack – Mobile app to Danalock device communications
CVE ID: Pending to be assigned
CVSS Score: 7.5

Status: Security update is available through a mobile app update. SDK update is available for integrators.

Affected Product

- Danalock mobile application below version 3.7.0 (Android) or 5.3.0 (iOS)

- Keaper mobile application below version 2.4.0 (Android) or 3.1.0 (iOS)

- Danalock mobile SDK below version 1.22.0 (Android) or 4.2.0 (iOS)

Fix Availability

An updated version of the mobile app has been published to Google Play Store and Apple App Store.

Users are advised to update their mobile applications as soon as possible.

No other mitigation actions are required.

Recommended Customer Actions

To keep systems secure:

1. Update any Danalock app to the latest version and ensure that automatic updates are turned on for the application in your app.

2. Update the Danalock SDK used in any mobile application integration to the latest version, then distribute.

SUPPORT

For assistance or questions related to the update, please reach out to Danalock support at danalocksupport@saltosystems.com

CREDIT

This vulnerability was discovered by Mnemonic

REVISION HISTORY

Version	1.0
Date	18/11/2026
Description	Initial publication of the security advisory

DISCLAIMER



Information in this security bulletin is provided for general guidance and informational purposes only, and reflects the information, analysis, and threat intelligence available to SALTO at the time of publication. That is, this document is provided “AS-IS”. It does not imply any guarantee, warranty, commitment, or undertaking of any kind, nor does it expand or modify the scope of any guarantee, warranty, or undertaking provided under any agreement to which a SALTO group or SALTO WECOSYSTEM companies are a party, including, without limitation, any implied warranties of merchantability, fitness for a particular purpose, or non-infringement.

While SALTO makes reasonable efforts to ensure that the information in this bulletin is accurate and relevant at the time of release, cybersecurity threats evolve continuously, and new vulnerabilities, techniques, or attack vectors may emerge that were not known, knowable, or reasonably foreseeable at the time of publication. Accordingly, SALTO does not guarantee that this security bulletin identifies or covers all potential security risks.

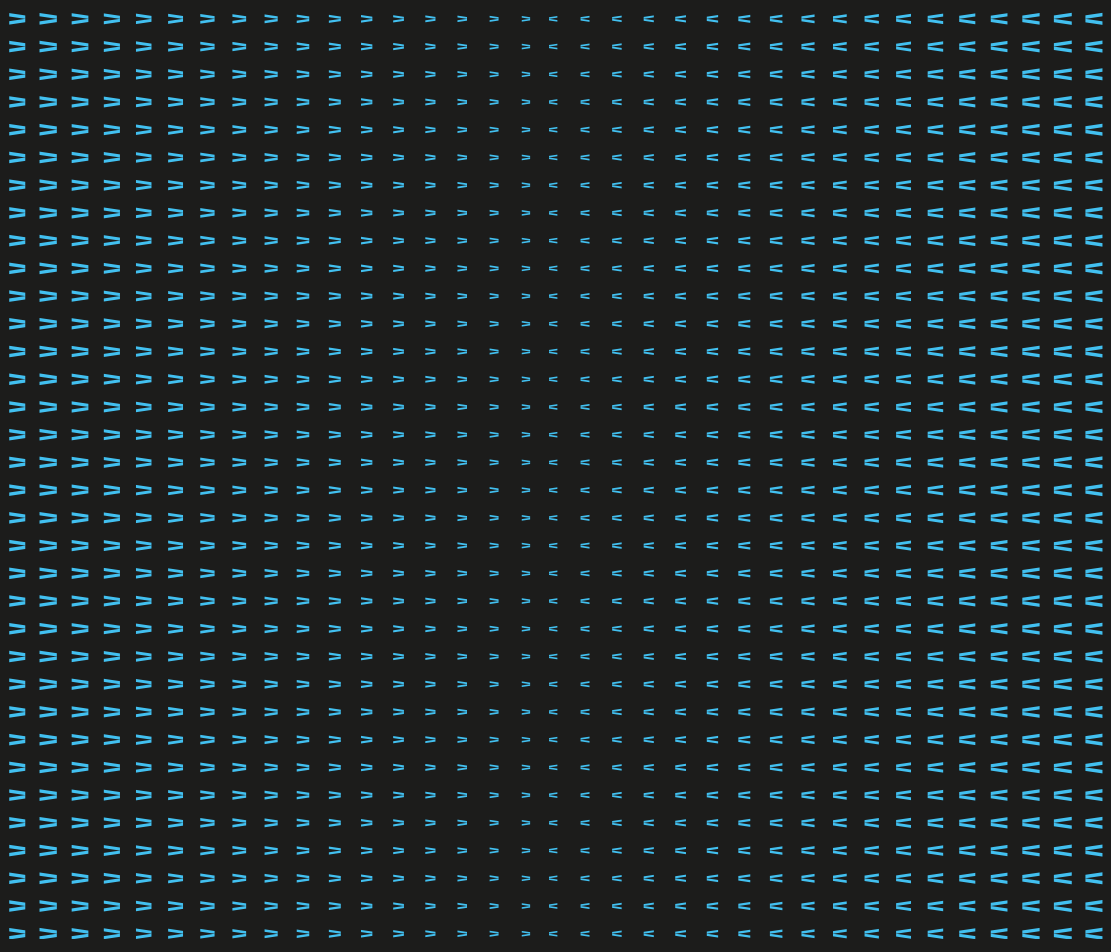
Any use of or reliance on the information contained in this document, or on any materials linked to or referenced by it, is at the user’s own risk. SALTO customers remain fully responsible for assessing the applicability of the guidance to their specific environments, as well as for implementing and maintaining appropriate technical and organizational security measures, including keeping all firmware and software up to date.

Except where required by applicable law or binding contractual obligations, SALTO shall not be liable for any direct, indirect, incidental, consequential, or other damages arising from or related to the use of, reliance on, or inability to use the information in this bulletin. SALTO reserves the right to modify, update, or withdraw this document at any time without prior notice.

For further information or inquiries, please contact SALTO.

salto

INSPIRED ACCESS



saltosystems.com

SALTO WECOSYSTEM