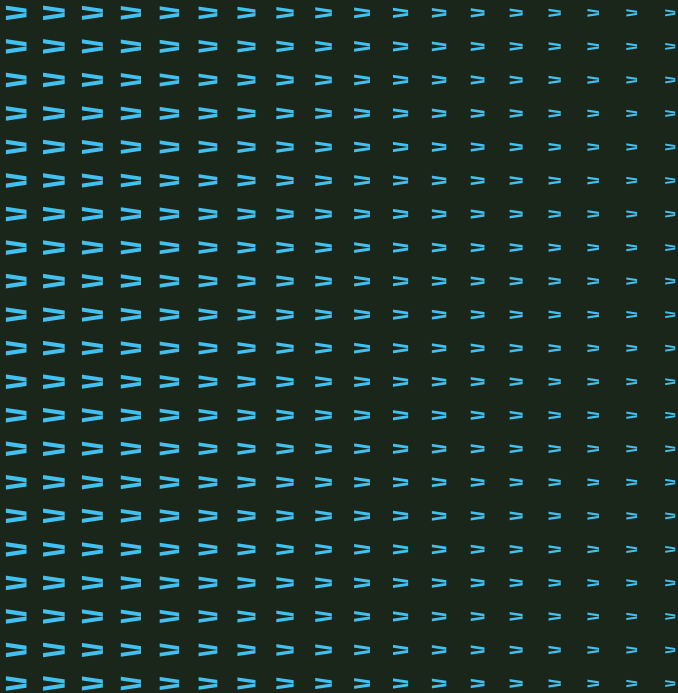


SECURITY ADVISORY

Salto Security Advisory Salto Space (Version 6.13.2.1)



Salto has released a security update for the on-premise Salto Space software that addresses an issue affecting installations where the logical partition (tenancy) feature is enabled.

In specific configurations, an authenticated operator with internal network access could perform certain privileged actions across logical partitions within the same installation.

There is no impact across different customers or deployments, and the issue cannot be exploited from the Internet when the system is installed following Salto best practices.

[Security Advisory](#)

SALTO SECURITY ADVISORY
SALTO SPACE

Salto Product Security Advisory

Product: Salto Space

Issue: Tenant Isolation – Cross Partition Privileged Actions

CVE ID: CVE-2026-11889

CVSS Score: 7.1

Status: Security Update Available in Version 6.13.2.1.

Published: 01/07/2026

Version: 1.0

Affected Product

Salto Space software before version 6.13.2.1

- Only installations using the **logical partition / tenancy** feature are affected
- Installations without partitioning enabled are **not affected**

Fix Availability

A security mitigation patch is available in version 6.13.2.1

- The update enforces stricter tenant isolation and **blocks cross-tenant execution of sensitive actions**, including:
 - > Door unlock commands
 - > Access-rights assignments
 - > Other privileged operations intended to remain tenant-restricted

All customers using the tenancy feature should upgrade to **version 6.13.2.1** as soon as possible.

Recommended Customer Actions

To further enhance security after applying the update:

1. Operate Salto Space on a protected internal network and avoid exposing it directly to the Internet.
2. Restrict operator-level accounts to the minimum required and apply least-privilege principles.
3. If feasible, disable the partitioning feature and operate under a single partition.
4. When strong tenant separation is required, consider running separate Salto Space instances (isolated environments) rather than relying solely on logical partitioning.

SUPPORT

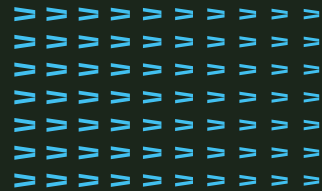
For assistance applying the update or reviewing your configuration, please contact your Salto representative or authorized partner.

CREDIT

This vulnerability was discovered by Limes Security

REVISION HISTORY

Version	1.0
Date	01/07/2026
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.

