RELEASE NOTE

Date: 11-Mar-24

Subject: Software changes, updates, bug fixes, etc.

Software: Fortanix Data Security Manager

Version: 4.19.2373

Fortanix, Inc. | 3910 Freedom Circle | Suite 104 | Santa Clara, CA 95052 | ☎ +1 650.943.2484
✉ info@fortanix.com
www.fortanix.com

OVERVIEW

This document provides an overview of bug fixes and known issues in the Fortanix Data Security Manager (DSM) SaaS 4.19.2373 release.

⚠ **WARNING**:

- You are **REQUIRED** to upgrade Fortanix DSM to version 4.13 or 4.16 before upgrading to version 4.19.2373. If you want to upgrade to 4.19.2373 from an earlier version, please reach out to the Fortanix Support team.
- Downgrading from Fortanix DSM version 4.19.2373 to any lower version is not possible.

NOTE:

- The Fortanix DSM cluster upgrade must be done with Fortanix Support on call. Please reach out to Fortanix Support if you are planning an upgrade.
- The customer's BIOS version must be checked by Fortanix Support prior to the Fortanix DSM software upgrade. If required, the BIOS version should be upgraded to the latest version and verified by Fortanix Support for a smooth upgrade.
- If your Fortanix DSM version is 4.13 or later, then the HSM Gateway version must also be 4.13 or later. Similarly, if the HSM Gateway version is 4.13 or later, then your Fortanix DSM version must be 4.13 or later.

BUG FIXES

- Fixed an issue where the DCAP peer certificates were not verified correctly **(JIRA: PROD-8321).**

  NOTE: Customers who have configured DCAP attestation on their cluster are advised to perform cluster master key (CMK) rotation after applying this patch.

RELEASE NOTE

Date: 11-Mar-24

Subject: Software changes, updates, bug fixes, etc.

Software: Fortanix Data Security Manager

Version: 4.19.2373

- Fixed VXLAN spoofing which allowed circumvention of host-based access controls to obtain administrative access on DSM nodes **(JIRA: DEVOPS-4607)**.

NOTE: We recommend customers operating clusters without attestation who have untrusted hosts on the same layer 2 network as their DSM hosts perform a CMK rotation after applying the patch.

For a complete list of new features, enhancements to existing features, other improvements, bug fixes, and known issues refer to the full description of the DSM 4.19 release note.

BEST PRACTICES

Because our quality assurance process includes continuous security testing, Fortanix recommends keeping all Fortanix products updated with the latest releases as soon as possible. As an overall strategy to reduce risk exposure, customers are encouraged to follow best practices, which include:

- Always keep the product version up to date.
- Only issue accounts to trusted administrators.
- Utilize strong passwords.
- Monitor logs.
- Enable daily backups for the cluster.

INSTALLATION

To download the DSM SGX (on-prem/Azure) and Software (AWS/Azure/VMWare) packages, click here.

SUPPORT

For any questions regarding this release note, please contact support@fortanix.com

RELEASE NOTE

Date: 11-Mar-24

Subject: Software changes, updates, bug fixes, etc.

Software: Fortanix Data Security Manager

Version: 4.19.2373

DISCLAIMERS

Fortanix and the Fortanix logo are registered trademarks of Fortanix, Inc. in the United States and other countries. All other trademarks are the property of their respective owners.

Fortanix assumes no responsibility for any inaccuracies in this document. Fortanix reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Copyright © 2024 Fortanix, Inc. All rights reserved.

Fortanix Data Security Manager Release Notes

Release 4.19.2373