RELEASE NOTE

Date: 16-May-22

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

Software: Fortanix Data Security Manager

Version: 4.6.2057

OVERVIEW

This document provides an overview of the resolved issues and known issues in the Fortanix Data Security Manager (DSM) 4.6.2057 release.

WARNING:

- It is "REQUIRED" to upgrade Fortanix DSM to version 4.3 or 4.4 before upgrading to version 4.6.2057. If you want to upgrade to 4.6.2057 from an older version, please reach out to the Fortanix Customer Success team.
- Before downgrading Fortanix DSM from version 4.6.2057 to older releases, remove all the IPv6 rules under the cluster IP-Policy setting.

NOTE:

- After the software package is uploaded, the expected time to upgrade a 3-node cluster is about 1.5 to 2 hours from version 4.3 or 4.4 to 4.6.2057.

BUG FIXES

1. Fixed an issue where the `GetAccountUsage` API had an incorrect session type **(JIRA: PROD-4610)**.
2. Fixed an issue where a JCE update to print `x-request-id` causes a backward compatibility error **(JIRA: PROD-4612)**.

SECURITY FIXES

- Fixed a bug where essential validation checks were missing when allocating and processing `FifoDescriptor` **(JIRA: PLAT-896)**. In a scenario where an attacker has complete control of the address space, an attacker could leverage these missing checks to rewrite the stack pointer outside of the enclave into an attacker-crafted stack. By utilizing ROP the attacker could execute arbitrary code and leak anything accessible by the enclave.

Fortanix, Inc. | 44 Castro St #305| Mountain View, CA 94041| +1 628.400.2043
info@fortanix.com
www.fortanix.com

RELEASE NOTE

Date: 16-May-22

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

Software: Fortanix Data Security Manager

Version: 4.6.2057

KNOWN ISSUES

- An account could be lost if account tables are inconsistent between nodes. Make sure a backup is successful before proceeding with ANY upgrade **(JIRA: PROD-4234)**.
- When a node is removed from a 3-node cluster with build 4.2.2087, and the 2-node cluster is upgraded with build 4.3.xxxx, it is possible that the deploy job is exited and marked completed before cluster upgrade (**JIRA: DEVOPS-2068**).

  Workaround: If all the pods are healthy, you can deploy the version again.
- The sync key API returns a "400 status code and response error" due to the short-term access token expiry during the sync key operation of a group linked to AWS KMS (**JIRA: PROD-3903**).
- `exclude` does not work in the `proxy` config for operations such as attestation (**JIRA: PROD: 3311**).

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.
- Restrict physical access to the appliance to trusted administrators.
- Create two System Administrator accounts.
- Enable daily backups for the cluster.

Fortanix, Inc. | 44 Castro St #305| Mountain View, CA 94041| ☎ +1 628.400.2043
✉ info@fortanix.com
🌐 www.fortanix.com

RELEASE NOTE

Date: 16-May-22

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

Software: Fortanix Data Security Manager

Version: 4.6.2057

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

DISCLAIMERS

Fortanix Data Security Manager Release Notes

Release 4.6.2057

Fortanix, Inc. | 44 Castro St #305| Mountain View, CA 94041| ☎ +1 628.400.2043

✉ info@fortanix.com

🌐 www.fortanix.com