Release Notes

HySecure security hotfix 5.2 build 5235

Last Updated: 1 March 2019

The information contained in this document represents the current view of Accops Systems Private Limited on the issues discussed as of the date of publication. Because Accops Systems Private Limited must respond to changing market conditions, it should not be interpreted as a commitment on the part of Accops Systems Private Limited. Accops Systems Private Limited cannot guarantee the accuracy of any information presented after the date of publication.

This white paper is for informational purposes only. ACCOPS SYSTEM PRIVATE LIMITED MAKES NO WARRANTIES, EXPRESSED OR IMPLIED IN THIS DOCUMENT.

Contact Accops Systems Private Limited.
Email: info@accops.com
Call: +91 9595 277 001

CONTENTS

OVERVIEW

This document outlines the vulnerabilities are fixed and how to apply hotfix HySecure gateway. It is recommended that apply this security hot fix on gateway version 5.0.

Note: Down time is required while apply this hot fix.

5.2.5235

Released on 1 March 2019

HOW TO APPLY HOTFIX

UPGRADE COMPATIBILITY OF HOTFIX V5.2.3.5

HySecure 5.2.3.5 hotfix is compatible with upgrades from the following HySecure versions only:

1. Upgrade existing installations based on HySecure 5.0 and running v5080
2. Upgrade existing installations based on HySecure 5.0 and running v5200
3. Upgrade existing installations based on HySecure 5.0 and running v5230

Please refer section Appendix A: Upgrading HySecure standalone gateway for procedures to upgrade HySecure gateway.

Please refer section Appendix B: Upgrading HySecure cluster for procedures to upgrade HySecure gateway.

HOW TO GET HYSECURE HOTFIX BUILD 5235

Download the HySecure upgrade patch:
https://propalmsnetwork-my.sharepoint.com/:u:/g/personal/support_accops_com/EeCUSHV4-U1IpAnLRyJfMT8BuCKx4nRmsVPZsSMDUgcAvw?e=1ppajt
MD5 Checksum of HySecure security hotfix: **53ba5edda43f8039c1d225ceadf1c4fc**

SECURITY ISSUES FIXED IN 5.2.5235

VULNERABILITIES IN OPENSSL FIXED.

OpenSSL **1.0.2k-8** is installed in HySecure 5230 and prior versions. This version of openSSL is vulnerable to multiple security flaws.

The flaws exist in the following scenarios:

- During key agreement in a TLS handshake using a DH(E) based cipher suite a malicious server can send a very large prime value to the client **(CVE-2018-0732)**.
- The OpenSSL RSA Key generation algorithm has been shown to be vulnerable to a cache timing side channel attack **(CVE-2018-0737)**.

Successful exploitation will allow a remote attacker: -

- To cause the client to spend an unreasonably long period of time generating a key for this prime resulting in a hang until the client has finished. This could be exploited in a Denial Of Service attack.
- With su-cient access to mount cache timing attacks during the RSA key generation process could recover the private key.

This security vulnerability has been fixed in this hot fix.

In This security hotfix following rpms are replaced.

- openssl-libs-1.0.2k-8.el7.x86_64 replaced with openssl-libs-1.0.2k-16.el7.x86_64
- openssl-1.0.2k-8.el7.x86_64 replaced with openssl-1.0.2k-16.el7.x86_64

APPENDIX A: UPGRADING HYSECURE STANDALONE SETUP

The section describes the detailed process to apply hotfix on HySecure standalone setup.
To apply hotfix on HySecure standalone gateway, follow these main steps:

- Login as security officer.
- Now go to "Upgrade Firmware" page under "Host Maintenance" Section => Select option ***Hotfix or service pack*** and upload the HySecure hotfix file.
- It may take 1 minutes or more to upload the hotfix based on network bandwidth between your PC and Gateway.
  Note: after this step, HySecure "fes" services will restart and all active user connections to this gateway will be disconnected.
- Once the hotfix file is uploaded and upgrade is started, the message will be displayed on the browser. In some cases, the message may not come on the management console. Refresh the browser and see if the upgrade has completed.
- After hotfix is applied successfully.
- Go to "Upgrade Firmware" page under "Host Maintenance" Section and click on ***View Logs*** button to check the hotfix installation logs.

APPENDIX B: UPGRADING HYSECURE CLUSTER

The section describes the detailed process to apply hotfix on HySecure Cluster having three nodes (Active, Standby and Real Gateway server):

To upgrade HySecure cluster, follow these main steps:

- Upgrade the HySecure Active Cluster Manger Node
- Upgrade the HySecure standby Cluster Manger Node
- Upgrade the HySecure Real Node

UPGRADING ACTIVE HYSECURE CLUSTER MANAGER NODE:

1. Connect to Active HySecure Cluster Manager node as Security Officer.

Note: Do not connect using Virtual IP Address, use the actual IP of Active node.

- Login as security officer.
- Now go to "Upgrade Firmware" page under "Host Maintenance" Section => Select option ***Hotfix or service pack*** and upload the HySecure hotfix file.
- It may take 1 minutes or more to upload the hotfix based on network bandwidth between your PC and Gateway.
  Note: after this step, HySecure "fes" services will restart and all active user connections to this gateway will be disconnected.
- Once the hotfix file is uploaded and upgrade is started, the message will be displayed on the browser. In some cases, the message may not come on the management console. Refresh the browser and see if the upgrade has completed.
- After hotfix is applied successfully.
- Go to "Upgrade Firmware" page under "Host Maintenance" Section and click on ***View Logs*** button to check the hotfix installation logs.

UPGRADING STANDBY HYSECURE CLUSTER MANAGER NODE:

2. Connect to Stanby HySecure Cluster Manager node as Security Officer.

Note: Do not connect using Virtual IP Address, use the actual IP of Standby node.

- Login as security officer.
- Now go to "Upgrade Firmware" page under "Host Maintenance" Section => Select option ***Hotfix or service pack*** and upload the HySecure hotfix file.
- It may take 1 minutes or more to upload the hotfix based on network bandwidth between your PC and Gateway.
  Note: after this step, HySecure "fes" services will restart and all active user connections to this gateway will be disconnected.
- Once the hotfix file is uploaded and upgrade is started, the message will be displayed on the browser. In some cases, the message may not come on the management console. Refresh the browser and see if the upgrade has completed.
- After hotfix is applied successfully.
- Go to "Upgrade Firmware" page under "Host Maintenance" Section and click on ***View Logs*** button to check the hotfix installation logs.

UPGRADING REAL HYSECURE CLUSTER NODE:

3. Connect to Real HySecure Cluster node as Security Officer.

Note: Do not connect using Virtual IP Address, use the actual IP of Real node.

- Login as security officer.
- Now go to "Upgrade Firmware" page under "Host Maintenance" Section => Select option ***Hotfix or service pack*** and upload the HySecure hotfix file.
- It may take 1 minutes or more to upload the hotfix based on network bandwidth between your PC and Gateway.
  Note: after this step, HySecure "fes" services will restart and all active user connections to this gateway will be disconnected.

- Once the hotfix file is uploaded and upgrade is started, the message will be displayed on the browser. In some cases, the message may not come on the management console. Refresh the browser and see if the upgrade has completed.
- After hotfix is applied successfully.
- Go to "Upgrade Firmware" page under "Host Maintenance" Section and click on ***View Logs*** button to check the hotfix installation logs.

About Accops

Accops Systems Private Limited. under “Accops” brand is a globally leading developer and provider of Enterprise Mobility solutions involving Application and Desktop Virtualization, Secure Remote Access and Privilege Access Management solutions.

Accops’ software and hardware products enable businesses to efficiently virtualize, secure and deliver business applications, corporate workspace and network services to their employees, partners, vendors, home users and mobile users, enabling instance access from anywhere using any device.

Tel: India +91 9595 277 001 | Europe +49 341 3315 78 30
Email: sales@accops.com | Web: www.accops.com