Release Notes

HySecure Security Hotfix-v5.2.3.6 (Linux Kernel's TCP SACK)

Last Updated: 19 August 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 HySecure security hotfix details.

Note: Down time is required while apply this hot fix on HySecure gateway. After apply this security hotfix gateway reboot the required.

HOW TO APPLY HOTFIX

UPGRADE COMPATIBILITY OF HOTFIX ACCOPS-HYSECURE-V5.2.3.6

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

1. Upgrade existing installations based on HySecure 5.0 and running v5200
2. 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 ACCOPS-HYSECURE-V5.2.3.6

Download the HySecure hotfix:
https://propalmsnetwork-my.sharepoint.com/:u:/g/personal/support_accops_com/EStGxZ_btH9EnCuZ9R--XlQB26IIZOKxwwpCydbwITgNeA?e=8V7ws7
MD5 Checksum of HySecure hotfix: **d8bf7bba9cb5c9e9596eb1dd3aaa6b91**

ACCOPS-HYSECURE-V5.2.3.6 (LINUX KERNEL'S TCP SACK) SECURITY HOTFIX DETAILS

Advisory ID: ACPS-SEC-12071901
CVE ID: CVE-2019-11477
Date Published: 12th July 2019
Severity: HIGH
Network Exploitable: YES
Public Exploits Available? : NO

Summary:

The TCP Selective Acknowledgement (SACK) module part of the Linux Kernel's TCP Stack is subject to an integer overflow flaw when handling TCP Selective Acknowledgements (SACKs). A remote attacker could exploit this flaw by send a specially crafted packet and cause a kernel panic which would cause the server to be non-operational and deny service to genuine users until the server is rebooted.

Affected Products:

ALL versions of Accops HySecure Gateway are affected by this vulnerability

Workarounds:

TCP Selective Acknowledgements (SACKs) can be disabled at the kernel level but this workaround is not advisable for servers accepting connections from the internet as it may cause severe performance impact especially in case of accessing HySecure's resources from a lossy network.

Fixes:

The integer overflow flaw has been corrected in the Linux Kernel and patches have been released publicly. Accops has released hotfix **5.2.3.6** to upgrade HySecure's kernel to the updated version. Customers are advised to apply this hotfix by contacting Accops Support.

Additional Links:

- https://www.cvedetails.com/cve/CVE-2019-11477/
- https://nvd.nist.gov/vuln/detail/CVE-2019-11477
- https://access.redhat.com/security/cve/cve-2019-11477

APPENDIX A: UPGRADING HYSECURE STANDALONE SETUP

The section describes the detailed process to upgrade HySecure standalone setup.
To upgrade 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.
- 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.
- Reboot HySecure gateway.

APPENDIX B: UPGRADING HYSECURE CLUSTER

The section describes the detailed process to upgrade 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.
- 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.
- Reboot the gateway

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.
- 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.
- Reboot the gateway

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.
- 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.
- Reboot the gateway

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