




User Guide for Fixing Security Vulnerability of Hybrid SAN

Before You Upgrade:





1. Applicability of the Patch:

This document instructs users to fix the CVE-2023-28808 security vulnerabilities of Hybrid SAN.

No.	Device Type	Controller Type	The included version range:
1	DS-A71024/48/72R	Single	<p>The scope of this patch is as follows:</p> <p>1) The scope of this patch covers from V2.3.4-2 to V2.3.8-8;</p> <p>2) For versions below V2.3.4-2, please contact HIK Technical Support Team for processing;</p> <p>3) For versions above V2.3.8-8, which have fixed this security vulnerability, and there is no need to upgrade this security patch package; *Checking the software version information by viewing on web login page: https://IP:2004</p> 
2	DS-A80624S	Single	
3	DS-A81016S	Single	
4	DS-A72024/72R	Single	
5	DS-A80316S	Single	
6	DS-A82024D	Dual	

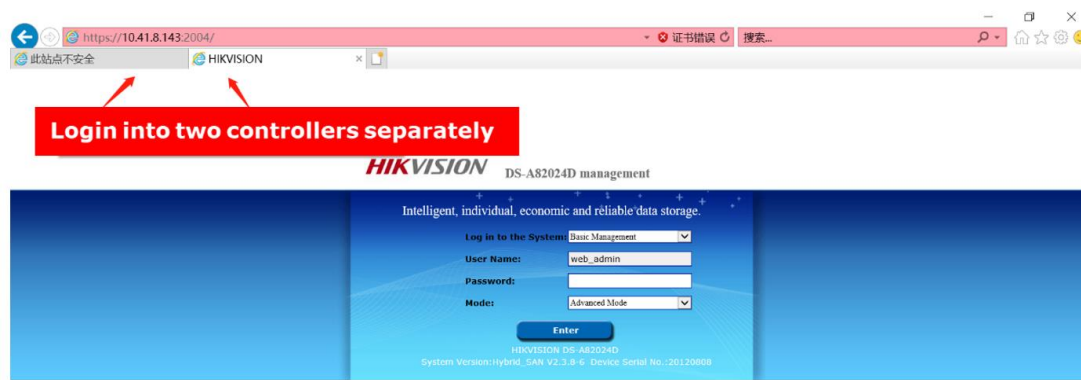
2. Please use **Internet Explorer** for upgrading.

3. There are 4 files in the package.

-  storos-step1-CheckMd5_for_CVR-V1.0-915
-  storos-step2-CVE-2023-28808_for_CVR_Update1-V1.0-915
-  storos-step3-CVE-2023-28808_for_CVR_Update2-V1.0-915
-  storos-step4-CVE-2023-28808_for_CVR_Update3-V1.0-915

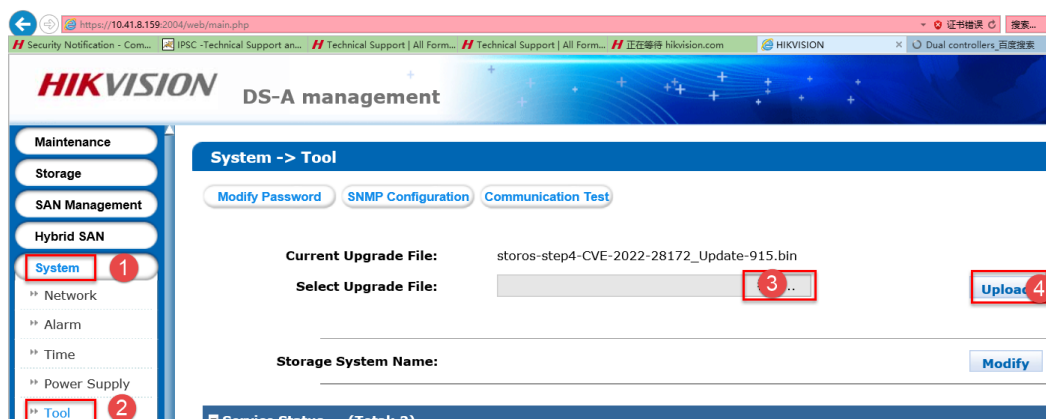
4. For dual controller device, please upgrade two controllers separately, and remember to do the upgrade one by one.

Notice: *If you forget the IP of dual controller device, please **contact HIK Technical Support Team**.*



Steps to Upgrade:

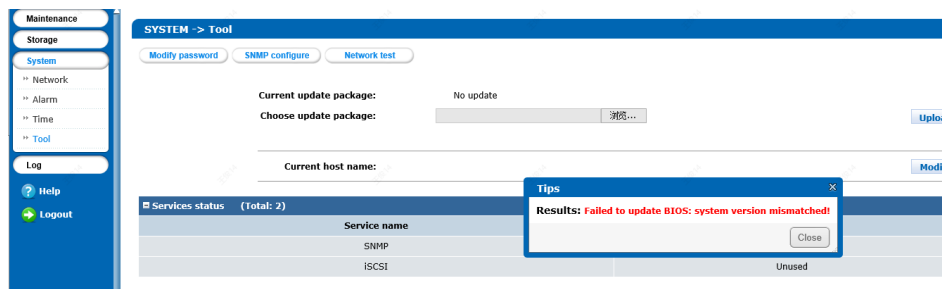
How to Upgrade: Login web page (https://IP:2004) and select **“System—Tool”** to reach the upgrade page as following Figure shown:



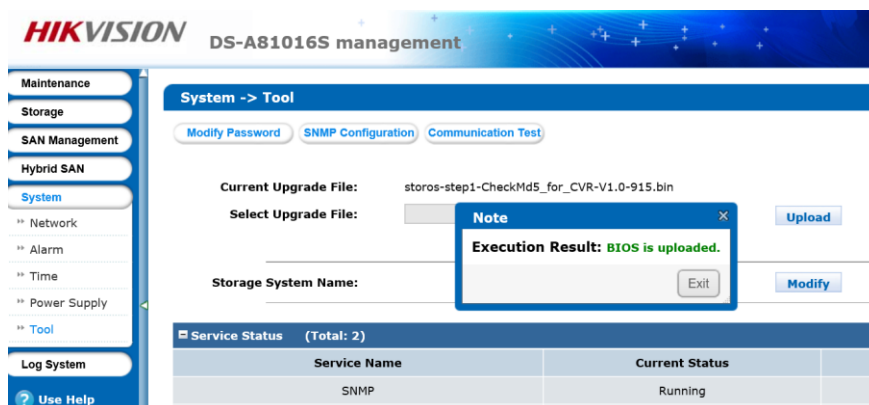
Step 1. Upgrade ① **“storos-step1-CheckMd5_for_CVR-V1.0-915.bin”** ;

- 1) If the upgrade fails, then please stop upgrading and **contact HIK Technical Support Team**.

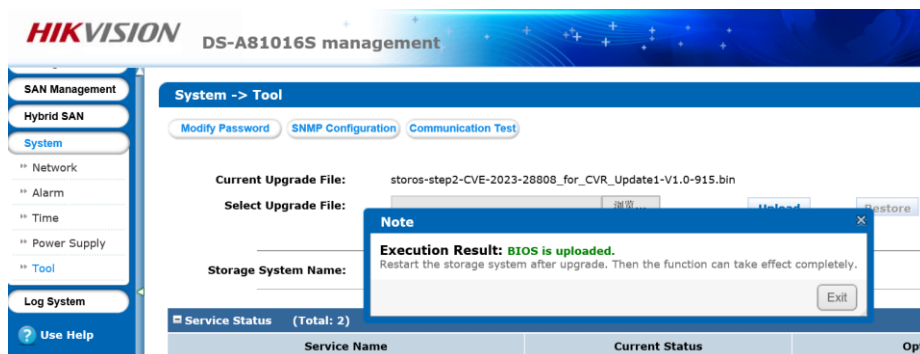
If the upgrade fails, which means that the Hybrid SAN have done some customization before, so you need to get the Customization Process Order (like DZP20220531204), then send it to a responsible Manager for Customization to evaluate a customized patch;



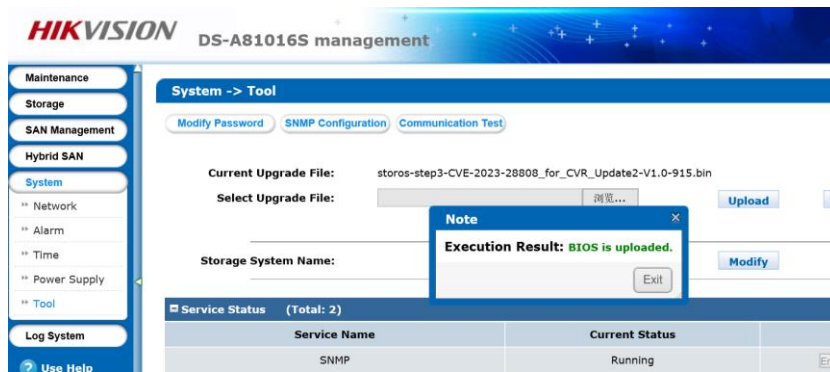
- 2) Or if the upgrade succeeds, then wait 2 minutes and continue the **Step 2**.



Step 2. Upgrade ② “*storos-step2-CheckVersion-915.bin*”, then wait 2 minutes;

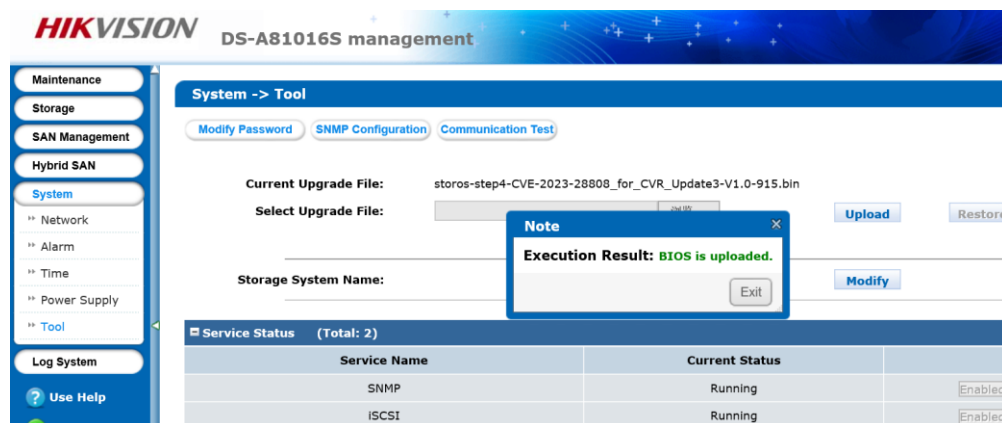


Step 3. Upgrade ③ “*storos-step3-CVE-2022-28171_Update-915.bin*”, then wait 2 minutes.



Tip: this patch may cause web logout, please wait some minutes, refresh page and re-login to continue;

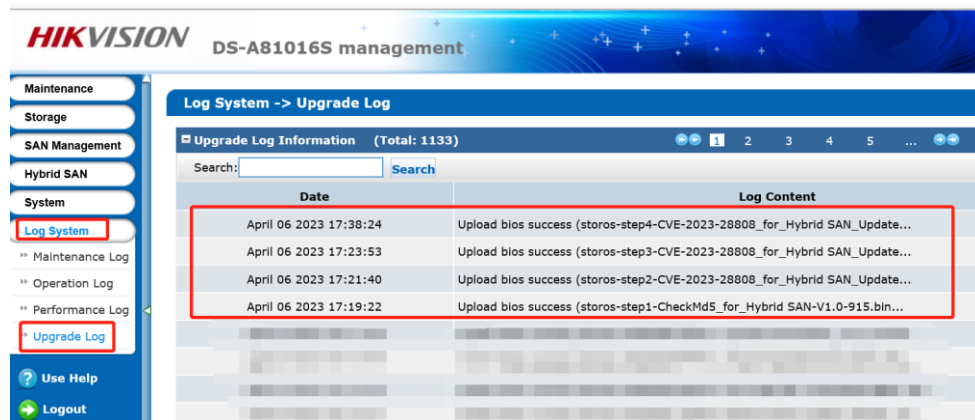
Step 4. Upgrade ④"storos-step4-CVE-2022-28172_Update-915.bin"



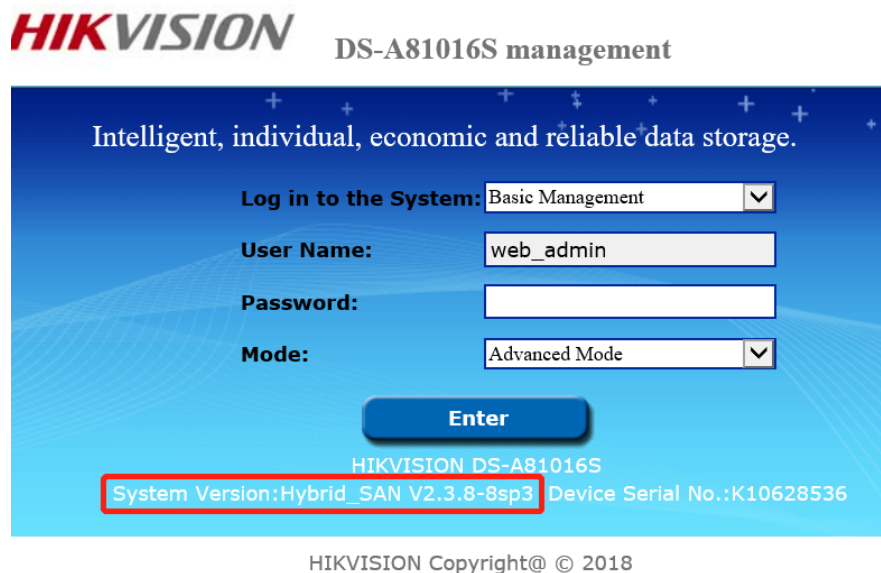
Confirm Upgrade Information:

After upgrading, enter "**Log System—Upgrade Log**":

- 1) If the latest log shown with 4 "**Upload bios success**", it means the upgrade is complete; **no need to reboot the device**;



- 2) Log out to the beginning 2004 page, to check whether the version ended with “sp3” after upload all 4 patches;



- 3) Then please check all the functions that used in your project and related with Hybrid SAN, such as recording and backup of video & picture, if there were any exceptions, please **contact HIK Technical Support Team**.

First Choice for Security Professionals

***HIK*VISION Technical Support**