

# Revised Hotfix Release Form

NIOS-99009 (General)

# Overview

Form Version Control.....	2
Resolution .....	2
Resolved.....	2
Details.....	2
Problem Summary.....	2
Hotfix Details.....	2
What to Expect.....	2
Member to Apply Hotfix .....	3
Application.....	3
Applying the Hotifx .....	3
Applying the Revert Hotfix .....	3
UI Validation.....	3
CLI Validation.....	4
Additional Considerations .....	4
Hotfix Precheck.....	4
Database Backup .....	4
Upgrades.....	4
Following Instructions.....	4

# Form Version Control

Version	Date	Updates
1	Feb 13, 2024	Hotfix Release Form Finalized
2	March 6, 2024	Revised Fix and information

## Resolution

### Resolved

## Details

### Problem Summary

The below CVE vulnerabilities are fixed by properly applying the version-specific Hotfix:

- CVE-2023-4408 - Parsing large DNS messages may cause excessive CPU load. This issue affects both authoritative servers and recursive resolvers.
- CVE-2023-5680 - Cleaning an ECS-enabled cache may cause excessive CPU load. If a resolver cache has a very large number of ECS records stored for the same name, the process of cleaning the cache database node for this name can significantly impair query performance.
- CVE-2023-50387 - Specially crafted DNSSEC signed zones can cause CPU exhaustion in validating resolvers.
- CVE-2023-50868 - Specially crafted queries into DNSSEC signed zones using NSEC3 can cause very high CPU consumption in validating resolvers.

### Hotfix Details

- This revised Hotfix resolves the security vulnerabilities related to CVE-2023-4408, CVE-2023-5680, CVE-2023-50387, CVE-2023-50868
- For the 8.6.2 hotfix, the matching CHF must first be installed within the Infoblox grid before the revised security fix can be applied. Please make sure to follow the CHF instructions precisely, as an appliance reboot may be required to fully install the CHF hotfix.
- The related Hotfix files and additional details can be found within KB#000009609
- Although this Hotfix should be applied to all members, a forced service restart only needs to be performed on those members currently running the DNS service. DNS service restarts can be performed on one member at a time to limit service impact.
- The **show upgrade\_history** CLI command can be run to determine which Hotfixes have already been applied to that member. If a related Hotfix is already applied to your grid (i.e. for the same NIOS version and feature), please consult with Infoblox Support before installing the new Hotfix.
- Before applying any Hotfix, we recommend gathering a Grid Database Backup.
- Please read through and follow the instructions provided within the Hotfix Release Form below.

### What to Expect

It's recommended to install the Hotfix on all grid members, but a force restart of DNS service is required only on DNS members.

## Member to Apply Hotfix

To Grid Master and all grid members

## Application

### Applying the Hotfix

**Note: It's important to follow the steps outlined below to ensure a successful Hotfix or Revert Hotfix installation.**

- 1) Download the Hotfix and Revert Hotfix files to a local workstation.
- 2) In the GUI, from the 'Grid' tab, select the **Upgrade** tab. Locate **Apply Hotfix** from the Toolbar and select the following from the dropdown: **To Grid Master and all Grid Members**.
- 3) In the **Apply Hotfix** dialog box, click **Select** and navigate to the Hotfix image file you want to upload. Click and **Upload** the Hotfix file.
- 4) Once the Hotfix is uploaded, a forced service restart on all DNS servers needs to be performed immediately. However, to mitigate impact, service restarts can be staggered, performed on one member at a time.
- 5) Navigate in the GUI to **Grid > Grid Manager > DNS**. From there, click the check box next to one of the members serving DNS. Under the **Toolbar** on the right, select **Restart Services**.
- 6) Change the radio button to **Force service restart** and then click the **Restart** button. Confirm prompts as needed.
- 7) Once service has been restored on that member, return to steps 5 and 6 above for the remaining members running DNS.


### Applying the Revert Hotfix

**Note: The Revert Hotfix is available to provide rollback flexibility as needed.**

- 1) Download the Hotfix and Revert Hotfix files to a local workstation.
- 2) In the GUI, from the 'Grid' tab, select the **Upgrade** tab. Locate **Apply Hotfix** from the Toolbar and select the following from the dropdown: **To Grid Master and all Grid Members**.
- 3) In the **Apply Hotfix** dialog box, click '**Select**' and navigate to the Hotfix image file you want to upload. Click and **Upload** the Hotfix file.
- 4) Once the Hotfix is uploaded, a forced service restart on all DNS servers needs to be performed immediately. However, to mitigate impact, service restarts can be staggered, performed on one member at a time.
- 5) Navigate in the GUI to **Grid > Grid Manager > DNS**. From there, click the check box next to one of the members serving DNS. Under the **Toolbar** on the right, select **Restart Services**.
- 6) Change the radio button to **Force service restart** and then click the **Restart** button. Confirm prompts as needed.
- 7) Once service has been restored on that member, return to steps 5 and 6 above for the remaining members running DNS.

### UI Validation

Verify that the Hotfix or Revert Hotfix has been successfully uploaded (**Grid > Upgrade >** under the **Hotfix** column, the **Last-Hotfix** should match the Hotfix name). If you see the below message, it may mean that the Hotfix was applied to a grid running an incompatible (for example, 8.6.3 with no Consolidated Hotfix already applied)

Upgrade to 8.6.3-51135-1241097029df completed	0 of 6 Members Completed
Hotfix	
 LAST-HOTFIX: Skipped Hotfix-8-6-3-NIOS-98724-APPLY-4cbc3ba40ea1270940acb2a22cf8d484-Sun-Feb-11-19-51-00-2024.bin   LAST-HOTFIX-TIME: Mon Feb 12 11:13:05 2024	

## CLI Validation

Confirm what software is currently running on the Grid / Grid Master

Infoblox > **show version**

Version : **8.6.1**-421683

SN : 564D49C8C935A8CFEF19263F3B554AEF

Hotfix : Hotfix-8-6-1-NIOS-87232-APPLY-4a57333b2cbea0d4aff166aa2edb38c6-Wed-Sep-14-00-07-47-2022.bin

Confirm that the Hotfix or Revert Hotfix was applied successfully

Infoblox > **show upgrade\_history**

REVERT version is: N/A

[2022/09/21 02:34:23] **Hotfix Hotfix-8-6-1-NIOS-87232-APPLY-4a57333b2cbea0d4aff166aa2edb38c6-Wed-Sep-14-00-07-47-2022.bin applied successfully**

## Additional Considerations

### Hotfix Precheck

The **show upgrade\_history** CLI command can be run to determine which Hotfixes have already been applied to that member. If a related Hotfix is already applied to your grid (i.e. for the same NIOS version and feature), please consult with Infoblox Support before installing the new Hotfix.

### Database Backup

Before applying any Hotfix, we recommend gathering a Grid Database Backup.

### Upgrades

It is Infoblox's expectation that the next grid software update will be to a release in which the issue is addressed.

Before upgrading to the next software release, please verify that the software version that you are upgrading to contains the final fix for this issue. This can be confirmed by searching the [NIOS Release Notes](#) of the newer software version for the respective fix (e.g. NIOS- 70673).

### Following Instructions

It is important that you complete all steps as instructed in this release form. Failure to comply with the instructions above may result in system errors. Infoblox will not be responsible or liable for issues arising from failure to comply with the provided instructions.



Infoblox unites networking and security to deliver unmatched performance and protection. Trusted by Fortune 100 companies and emerging innovators, we provide real-time visibility and control over who and what connects to your network, so your organization runs faster and stops threats earlier.

Corporate Headquarters  
2390 Mission College Blvd, Ste. 501  
Santa Clara, CA 95054  
+1.408.986.4000  
[www.infoblox.com](http://www.infoblox.com)