RELEASE NOTES

NIOS 8.6.3.3

Consolidated Hotfix-3

Table of Contents

Introduction 2
Important Guidelines 2
Hotfix Details 2
Before Applying the Hotfix 3
Applying the Hotfix 3
Applying the Revert Hotfix 4
Validating the Hotfix 5
Addressed Vulnerabilities 6
Issues Fixed in NIOS 8.6.3.3 Consolidated Hotfix-3 7
Issues Fixed in NIOS 8.6.3.2 Consolidated Hotfix-2 9
Issues Fixed in NIOS 8.6.3.1 Consolidated Hotfix-1 9
Known General Issues 10

Introduction

The Infoblox NIOS 8.6.3.3 Consolidated Hotfix-3 release is a consolidated release that includes important bug fixes identified since the release of NIOS 8.6.3.

Important Guidelines

The 8.6.3.3 consolidated hotfix can be applied on both the active NIOS 8.6.3 version, or on the Grid in which the NIOS 8.6.3 version is in the "In Distribution Complete" stage.

IMPORTANT:

- **PLEASE NOTE: It is important that you complete all steps as instructed in the hotfix release form; failure to comply with the instructions may result in system errors. While we strive to support all our customers, we cannot be held responsible for issues that arise due to deviations from the provided hotfix instructions. You can view the hotfix release form in the KB article published to announce the hotfix release.**
- If you have applied a custom hotfix for NIOS 8.6.3, contact Infoblox support before applying NIOS 8.6.3.*x* consolidated hotfixes.

Hotfix Details

The following are the details of the hotfix:

Hotfix Name

Hotfix-CHF-8.6.3.3-J96954-Apply-838b667604f8eb85215047e657168c64-Wed-Feb-28-08-49-23-2024.bin

Hotfix SHA256SUM

8f930874e5c415f11e6d894df6b4ed18aa36d5b26ffe04676c7aba8358d10af5

Revert Hotfix Name

Hotfix-CHF-8.6.3.3-J96954-Revert-8c6caacd1f3cf638a55ded681a3a79e1-Fri-Feb-23-08-10-55-2024.bin

Revert Hotfix SHA256SUM

eeb91840aa3fd0f5d5dd5cd4d1c07626dd27587ccdc340fd12d1d28a9ce13ad1

Before Applying the Hotfix

- Infoblox recommends that you take a database backup as a precautionary measure before installing the hotfix.
- You can apply the hotfix on physical appliances; however, Infoblox does not recommend applying X6 series licenses on those appliances.
- The NIOS license will be removed if you apply the revert hotfix on the node that has the X6 series license installed after applying the hotfix. This applies if you have:
    - Installed NIOS 8.6.3 > applied consolidated hotfix 2 > applied consolidated hotfix 3 > reverted consolidated hotfix 3 > reverted consolidated hotfix 2
    - Installed NIOS 8.6.3 > applied consolidated hotfix 3 > reverted consolidated hotfix 3
- If you have applied a custom hotfix for NIOS 8.6.3, contact Infoblox support before applying NIOS 8.6.3.x consolidated hotfixes.
- For detailed information about mapping X6 series virtual licenses installed on X5 virtual appliances running NIOS 8.6.3 with X6 series licenses after upgrading to NIOS 9.0.2, see KB article number 000009433, "Behavior of X6 Series virtual licenses installed on X5 virtual appliances after upgrading to NIOS 9.0.2".

Applying the Hotfix

Perform the following steps to apply the hotfix:

1. Download the hotfix file to a local workstation.
2. In Grid Manager, from the **Grid** tab, select the **Upgrade** tab.
3. Locate **Apply Hotfix** from the Toolbar and select the **To Grid Master** and **All Grid Members** options from the drop-down list.
4. In the *Apply Hotfix* dialog box, click **Select** and navigate to the hotfix image file that you downloaded.
5. Upload the hotfix file.
6. Run the `show action_to_activate_hotfix` CLI command to view the best-suggested action to activate the hotfix.
   For example, `show action_to_activate_hotfix infoblox.localdomain`
   NOTE: This CLI command is available from NIOS version 8.6.3 and it can be run only on the Grid Master. **This command only lists what you need to do to complete applying the hotfix. It does not list whether you have completed it or not.**
7. If the hotfix is applied at the distribution complete stage, no action is required to activate the hotfix.

After applying the hotfix in the active NIOS 8.6.3 version, perform an appliance reboot on all the nodes on which the hotfix has been applied, to activate the changes.

NOTE:

- The consolidated hotfix application may fail in the alternate partition at the distribution complete stage for Trinzic appliances. If it fails, re-apply the hotfix after upgrading.
- You can apply the hotfix after distributing NIOS 8.6.3. After an upgrade, the hotfix will be in effect without the need of an additional restart.
- If the FIPS mode is enabled, you must wait until the integrity checksum file is generated, then reboot the appliance for all the changes to be reflected.
- The notes in this section also apply to the revert hotfix.

Applying the Revert Hotfix

Apply the revert hotfix only if you run into an issue when applying the consolidated hotfix. Infoblox recommends that you contact Infoblox Support if you think you need to revert but are not sure.

Perform the following steps to apply the revert hotfix:

1. Download the revert hotfix file to a local workstation.
2. In Grid Manager, from the **Grid** tab, select the **Upgrade** tab.
3. Locate **Apply Hotfix** from the Toolbar and select the **To Grid Master** and **All Grid Members** options from the drop-down list.
4. In the *Apply Hotfix* dialog box, click **Select** and navigate to the hotfix image file that you downloaded.
5. Upload the revert hotfix file.
6. Run the `show action_to_activate_hotfix` CLI command to view the best suggested action to activate the hotfix.
   For example, `show action_to_activate_hotfix infoblox.localdomain`
   NOTE: This CLI command is available from NIOS version 8.6.3 and it can be run only on the Grid Master. **This command only lists what you need to do to complete applying the hotfix. It does not list whether you have completed it or not.**
7. If the hotfix is reverted in the distribution complete stage, no action is required to revert the hotfix.

After reverting the hotfix in the active NIOS 8.6.3 version, perform an appliance reboot on all the nodes on which the revert hotfix has been applied, to revert the changes.

Validating the Hotfix

CLI Validation

Run the following commands to validate the hotfix using the NIOS CLI:

```
Infoblox > show upgrade_history

REVERT version is: N/A

[2024/02/28 04:24:39] Hotfix Hotfix-CHF-8.6.3.3-J96954-Apply-
838b667604f8eb85215047e657168c64-Wed-Feb-28-08-49-23-2024.bin applied
successfully

[2024/02/28 05:03:03] Hotfix Hotfix-CHF-8.6.3.3-J96954-Revert-
8c6caacd1f3cf638a55ded681a3a79e1-Fri-Feb-23-08-10-55-2024.bin applied
successfully

Infoblox > show action_to_activate_hotfix infoblox.localdomain

Hotfix generic name: CHF-8.6.3.3-J96954-apply-1708656371

Hotfix time: 23-02-24 02:46:11 UTC

Suggested best action to activate: Appliance reboot required.

Member status: ONLINE

Note: This action is to be performed after applying the hotfix, if already
done please ignore.
```

UI Validation

To verify that the hotfix or revert hotfix has been successfully uploaded in Grid Manager:

1. Navigate to **Grid** > **Upgrade** tab.
2. In the **Hotfix** column, the **Last Hotfix** field must match the hotfix name.

Addressed Vulnerabilities

This section lists security vulnerabilities that were addressed in this release. For additional information about these vulnerabilities, including their severities, please refer to the National Vulnerability Database (NVD) at https://nvd.nist.gov/. The Infoblox Support website at https://support.infoblox.com also provides more information, including vulnerabilities that do not affect Infoblox appliances.

CVE-2023-50868

The Closest Encloser Proof aspect of the DNS protocol (in RFC 5155 when RFC 9276 guidance is skipped) allows remote attackers to cause a denial of service (CPU consumption for SHA-1 computations) via DNSSEC responses in a random subdomain attack, aka the "NSEC3" issue. The RFC 5155 specification implies that an algorithm must perform thousands of iterations of a hash function in certain situations.

CVE-2023-50387

Certain DNSSEC aspects of the DNS protocol (in RFC 4033, 4034, 4035, 6840, and related RFCs) allow remote attackers to cause a denial of service (CPU consumption) via one or more DNSSEC responses, aka the "KeyTrap" issue. One of the concerns is that, when there is a zone with many DNSKEY and RRSIG records, the protocol specification implies that an algorithm must evaluate all combinations of DNSKEY and RRSIG records.

CVE-2023-5680

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. This issue affects BIND 9 versions 9.11.3-S1 through 9.11.37-S1, 9.16.8-S1 through 9.16.45-S1, and 9.18.11-S1 through 9.18.21-S1.

CVE-2023-4408

The DNS message parsing code in `named` includes a section whose computational complexity is overly high. It does not cause problems for typical DNS traffic, but crafted queries and responses may cause excessive CPU load on the affected `named` instance by exploiting this flaw. This issue affects both authoritative servers and recursive resolvers. This issue affects BIND 9 versions 9.0.0 through 9.16.45, 9.18.0 through 9.18.21, 9.19.0 through 9.19.19, 9.9.3-S1 through 9.11.37-S1, 9.16.8-S1 through 9.16.45-S1, and 9.18.11-S1 through 9.18.21-S1.

Issues Fixed in NIOS 8.6.3.3 Consolidated Hotfix-3

ID	Severity	Summary
NIOS-98326	Critical	The CVE-2023-4408 and CVE-2023-5680 vulnerabilities were not addressed.

ID	Severity	Summary
NIOS-99358	Major	After a hotfix was applied, BIND restarted twice causing service delays.
NIOS-99081	Major	After a hotfix installation, the Grid Manager kept logging out users.
NIOS-98772	Major	The CVE-2018-11409 vulnerability was not addressed.
NIOS-98771	Major	During a product restart or reboot, the Splunk PID was not registered with the process manager.
NIOS-98771	Major	The CVE-2023-50868 vulnerability was not addressed.
NIOS-98748	Major	Under certain circumstances, the DNS server stopped responding to queries.
NIOS-98569	Major	Unable to restore a backup file that contained several DNS Traffic Control objects on a TE-815 appliance.
NIOS-98548	Major	System-generated records were randomly deleted from DNS zones.
NIOS-98247	Major	Syslog support needed to be added when the fast path cores were stuck.
NIOS-98131	Major	Details and logs were not available to diagnose the cause of the CPU getting locked.
NIOS-98130	Major	Under certain circumstances, fast path CPUs got stuck.
NIOS-98031	Major	After a NIOS upgrade, loading the Grid Manager dashboard took a long time.
NIOS-97933	Major	Under certain circumstances, static data collection resulted in large memory consumption and caused API issues.
NIOS-97911	Major	Unable to run the advanced global search in Grid Manager.

NIOS-97885	Major	DNS resolution intermittently failed for one of the DNS Traffic Control servers.
NIOS-97867, NIOS-96983	Major	After a NIOS upgrade, the DNS Traffic Control screens were sluggish to navigate.
NIOS-97782	Major	A SafeNet session had issues that caused crypto failures during HSM zone signing operations.
NIOS-97046	Major	Unable to delete a filter and a message displayed that the filter was assigned to a network; however, the filter was not assigned to the specified network.
NIOS-97043	Major	The HSM firewall needed to be fixed to ensure that proper SNAT rules for HSM were added when the Grid Master was in HA mode while configuring HSM.
NIOS-97012	Major	The **Cloud** > **Networks** screen and the **Cloud** > **Tenants** > <*tenant_name*> > **Networks** screen were slow to load and did not display data.
NIOS-97000	Major	In an LBDN pool, the IP address of a DNS server whose status was marked as "Down" was being returned.
NIOS-96980	Major	A delay option was required to be added to aid the disaster recovery scenario during a Grid Master Candidate promotion.
NIOS-96953	Major	Under certain circumstances, a Splunk version disclosure occurred on the Advanced DNS Protection (external DNS) members.
NIOS-96909	Major	The **Delay between Restart Groups** and **Member Restart Timeout** fields in the *Grid DNS Properties* > **Restart** tab did not work as expected.
NIOS-95864	Major	Unable to view the audit log and an error message was displayed.
NIOS-95158	Major	When an ACL was assigned to an authentication group, API calls responded with an internal error.
NIOS-94884	Major	Unable to add new values to the Site_ID extensible attribute, and the values already present did not load and displayed blank spaces.

Issues Fixed in NIOS 8.6.3.2 Consolidated Hotfix-2

ID	Severity	Summary
NIOS-96835	Major	Invalid records were being cached when fault tolerant caching was enabled.
NIOS-96432	Major	After reclaiming a set of IP addresses, a database synchronization issue occurred in the Grid members.
NIOS-96013	Major	The DNS over HTTPS configuration (DoH) debug prints needed to be removed because they were hindering performance numbers.
NIOS-95945	Major	AD authentication with nested groups failed after a NIOS upgrade.
NIOS-95827	Major	The X6 series virtual license support was required for NIOS 8.6.3.
NIOS-94892	Major	The libnl3 package had to be upgraded from libnl3-3.2.21-2 to libnl3-3.2.28-4 due to a memory leak in the libnl3-3.2.21 package.

Issues Fixed in NIOS 8.6.3.1 Consolidated Hotfix-1

ID	Severity	Summary
NIOS-95047	Critical	AWS Route 53 synchronization stopped using the configured proxy server after an upgrade.

ID	Severity	Summary
NIOS-95162	Major	Under certain circumstances, a high number of zone transfers with the same serial number occurred.
NIOS-95161	Major	Unable to view and export alias records after a NIOS upgrade.
NIOS-95159	Major	A WAPI search call returned an unknown argument/field “ipv4addrs”.
NIOS-95029	Major	The public_suffix_list.dat file did not get downloaded due to a certificate issue.

NIOS-95028	Major	When the **VPN over the MGMT** option was enabled on an AWS Grid member, the AWS Grid member was not able to connect back to Grid Master.
NIOS-94950	Major	After a NIOS upgrade, certain CA certificates did not work as expected.
NIOS-94829	Major	Name server groups were not added to the allow-query list for RPZ zones.
NIOS-94082	Major	Under certain circumstances, the system swap space usage exceeds the critical threshold value.

Known General Issues

ID	Severity	Summary
NIOS-95839	Major	Application of the consolidated hotfix may fail on the alternate partition in the distribution complete stage for Trinzic appliances. **Workaround:** If the consolidated hotfix application fails in the alternate partition in the distribution complete stage, reapply the hotfix after upgrading.

infoblox.

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