RELEASE NOTES

NIOS 8.6.2.4
Consolidated Hotfix-4

Table of Contents

Introduction

The Infoblox NIOS™ 8.6.2.4 Consolidated Hotfix-4 release is a consolidated release that includes bug fixes in the current hotfix-4 release as well as bug fixes in the NIOS 8.6.2 consolidated hotfix-1, hotfix-2, and hotfix-3 releases.

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.

Hotfix Details

The following are the details of the hotfix:

Hotfix Name

Hotfix-CHF-8.6.2.4-J91437-Apply-ed88048cb1d0ae0e09ff9e4ca9ee2204-Sun-Jul-23-17-50-44-2023.bin

Hotfix SHA256SUM

41bfe16770d951003decce8d27ed5a9dc02da41af463970a18426edf16079902 Hotfix-CHF-8.6.2.4-J91437-Apply-ed88048cb1d0ae0e09ff9e4ca9ee2204-Sun-Jul-23-17-50-44-2023.bin

Revert Hotfix Name

Hotfix-CHF-8.6.2.4-J91437-Revert-2944188f24482bb912b4b575df2bc660-Thu-Aug-17-20-55-18-2023.bin

Revert Hotfix SHA256SUM

7456de5688e1737afd7f446f2bd9e3cad09ae88d19c3c91bfc412e301d22ba5c

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.

After applying the hotfix, perform an appliance reboot on all the nodes that the hotfix has been applied to, to activate all the changes.

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.

After reverting the hotfix, perform an appliance reboot on all the nodes that the revert hotfix has been applied to, 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
[2023/08/18 17:23:27] Hotfix Hotfix-CHF-8.6.2.4-J91437-Apply-
ed88048cb1d0ae0e09ff9e4ca9ee2204-Sun-Jul-23-17-50-44-2023.bin applied successfully
[2023/08/18 17:31:36] Hotfix Hotfix-CHF-8.6.2.4-J91437-Revert-
2944188f24482bb912b4b575df2bc660-Thu-Aug-17-20-55-18-2023.bin applied successfully
```

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 Consolidated Hotfix-2 release, and BIND and OpenSSL related vulnerabilities addressed in Consolidated Hotfix-4 release. For vulnerabilities that are not listed in this section, refer to Infoblox KB #2899. For additional information about these vulnerabilities, including their severities, please refer to the National Vulnerability Database (NVD) at http://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-2023-2828

The effectiveness of the cache-cleaning algorithm used in a recursive resolver to keep the memory use below the configured limit can be severely diminished by querying the resolver for specific RRsets in a certain order, allowing the configured `max-cache-size` limit to be significantly exceeded.

CVE-2023-0215

This vulnerability was found in OpenSSL's BIO_new_NDEF function used for upstreaming ASN.1 data through a BIO. Under certain conditions. For example, if a CMS recipient public key is invalid, the function instead of returning a new filter BIO to the caller, frees the BIO and returns a NULL result indicating a failure. If the caller then goes on to call BIO_pop() on the BIO, a use-after-free will occur, which most likely results in a crash.

CVE-2023-0286

This vulnerability is relating to the OpenSSL X.400 address processing inside an X.509 GeneralName. When the certificate revocation list (CRL) checking is enabled, the vulnerability allows an attacker to pass arbitrary pointers to a memcmp call, enabling them to read memory contents or enact a denial of service. The vulnerability is most likely to only affect applications that have implemented their own functionality for retrieving CRLs over a network.

CVE-2023-4304

A timing-based side channel exists in the OpenSSL RSA Decryption implementation that an attacker can use to recover a ciphertext across a network.

CVE-2022-3488

Processing of repeated responses to the same query, where both responses contain ECS pseudo-options, but where the first is broken in some way, can cause BIND to exit with an assertion failure.

CVE-2022-38178, CVE-2022-38177

By spoofing the target resolver with responses that have a malformed ECDSA signature, an attacker can trigger a small memory leak. It is possible to gradually erode available memory to the point where named crashes for lack of resources.

CVE-2022-2929

In ISC DHCP 1.0 -> 4.4.3, ISC DHCP 4.1-ESV-R1 -> 4.1-ESV-R16-P1 a system with access to a DHCP server, sending DHCP packets crafted to include fqdn labels longer than 63 bytes, could eventually cause the server to run out of memory.

CVE-2022-2928

In ISC DHCP 4.4.0 -> 4.4.3, ISC DHCP 4.1-ESV-R1 -> 4.1-ESV-R16-P1, when the function option_code_hash_lookup() is called from add_option(), it increases the option's refcount field. However, there is not a corresponding call to option_dereference() to decrement the refcount field. The function add_option() is only used in server responses to lease query packets. Each lease query response calls this function for several options, so eventually, the reference counters could overflow and cause the server to abort.

CVE-2022-2795

By flooding the target resolver with queries exploiting this flaw an attacker can significantly impair the resolver's performance, effectively denying legitimate clients access to the DNS resolution service.

CVE-2021-20322

A flaw in the processing of received ICMP errors (ICMP fragment needed and ICMP redirect) in the Linux kernel functionality was found to allow the ability to quickly scan open UDP ports. This flaw allows an off-path remote user to effectively bypass the source port UDP randomization. The highest threat from this vulnerability is to confidentiality and possibly integrity, because software that relies on UDP source port randomization are indirectly affected as well.

Issues Fixed in NIOS 8.6.2.4 Consolidated Hotfix-4

ID	Severity	Summary
NIOS-93255	Critical	NIOS was vulnerable to CVE-2023-2828.
NIOS-90554	Critical	NIOS was possibly vulnerable to CVE-2023-0286, CVE-2022-4304, CVE-2023-0215, CVE-2022-4450, CVE-2023-0464, CVE-2023-0465, and CVE-2023-0466.
NIOS-90485	Critical	The backup files of DNS stats not getting deleted caused a gradual increase in disk space usage on some servers.
NIOS-89982	Critical	Memory leak caused the memory usage on Grid Master to increase gradually.
NIOS-86977	Critical	The incorrect `DNS_RDATATYPE_FORMATSIZE` that had the potential to cause problems involving stack and heap usage, needed to be fixed.
NIOS-60625	Critical	Unable to restart the DNS service from Grid Manager. When **Grid Manager** > **Member** tab was clicked, "An error has occurred. Contact technical support if the problem persists." was displayed.

ID	Severity	Summary
NIOS-94359	Major	After an upgrade from NIOS 8.5.4 to 8.6.2, WAPI calls intermittently returned “Unknown argument/field: 'ipv4addrs“ in the response.
NIOS-92795	Major	The passive node of the Grid Master was restarting every four hours after four of the LBDN records were disabled.
NIOS-92653	Major	DNSTAP caused the protobuf-c module to crash.
NIOS-92009	Major	Unable to add a second partition to the newly created Luna HSM group due to issue with reading the group number in the output logs.
NIOS-90975	Major	The output of the `show interface all` command did not show the configured IPv4 loopback address.
NIOS-90854	Major	Importing Keyset in an IDN zone was failing although the keyset belonged to the subzone of the zone to which it was imported.
NOS-90483	Major	Some of the Grid members were not forwarding ADP data to the reporting appliance though they had ADP hits.
NIOS-90410	Major	The DNS server was restarting every 1 to 2 minutes as the resolver on the NIOS resolver/DFP host stopped responding to queries at random times.
NIOS-90278	Major	OpenSSL version needed to be upgraded to 1.1.1t due to certain common vulnerabilities.
NIOS-89726	Major	"name.SIGQUIT" cores were observed while performing multiple operations on a member in a very-large-running-tasks Grid.
NIOS-89475	Major	The fp-rte binary was using Linux host OS OpenSSL libraries instead of 6windgate OpenSSL libraries causing an impact on the DCA functionality.
NIOS-88034	Major	The start of authority (SOA) serial number in DNS notifies that were sent from the lead secondary in syslog were out of sync with those in traffic captures.
NIOS-87298	Major	IB-FLEX caching servers running on OpenStack had issues with responding to queries from certain domains.
NIOS-86391	Major	The DNSSEC zone became invalid because the RRSIG for the DNSKEY RRSET was not being updated.

ID	Severity	Summary
NIOS-86266	Major	The DNS Query Rate by Query Type (detailed) report was not showing any data.
NIOS-86180	Major	A DNS server was restarting repeatedly while configuring Response Policy zones and had issues that caused core dumps.
NIOS-84612	Major	DNSSEC signed records had intermittent DNSSEC validation issues when the Smart Cache feature was turned on.
NIOS-84480	Major	High DB utilization rendered the Grid Master in a HA configuration to be intermittently unresponsive causing the GUI to be inaccessible.

ID	Severity	Summary
NIOS-93658	Minor	Need to revert the tcp flow time out configs to original 8.6.2 values.
NIOS-89706	Minor	When an appliance configured as a forward-only server returned SERVFAIL for a query, the serverquota counter increased even though fetches-per-server was disabled.
NIOS-88135	Minor	The Alias A record was not moving to the newly created sub zone automatically. The record had to be updated to move it.
NIOS-84457	Minor	When importing large files, a CSV Import job stopped responding with its status as 'Import in Progress'.
NIOS-83171	Minor	Secure updates for GSS-TSIG were logged in syslogs even though the GSS-TSIG configuration was disabled.

Issues Fixed in NIOS 8.6.2.3 Consolidated Hotfix-3

ID	Severity	Summary
NIOS-90151	Major	UDPv4 errors were being displayed in the log files and DNS queries including health checks and load balancer queries were not being responded to.
NIOS-89996	Major	After a hotfix installation, running the `tcpdump` command displayed an error message.

ID	Severity	Summary
NIOS-89889	Major	Server failure responses from authoritative servers were displayed intermittently in the log files.
NIOS-89806	Major	After a DNS outage, SmartNIC logs needed to be analyzed.
NIOS-89434	Major	The DNS service crashed after recursive lookups exceeded the threshold value.
NIOS-88970	Major	A WAPI search for an object whose extensible attribute is an inherited value returned an error.
NIOS-88900	Major	Under certain circumstances, a DNS service disruption occurred and DNS was unavailable on some Grid members for several hours.
NIOS-88866	Major	Idendtity Provider (IdP) metadata calls against NIOS failed due to a certificate path mismatch.
NIOS-88674	Major	Under certain circumstances, all DNS secondary nodes went offline and frequent product restarts took place.
NIOS-87768	Major	NXDOMAIN response deprioritization settings were not updated correctly for Grid members when the override option was selected.
NIOS-87745	Major	The DNS server was dropping DNS requests from an ADP rule.
NIOS-87236	Major	After a NIOS upgrade, the *Grid Member Properties Editor* > **General** > **Basic** screen displayed an internal error.
NIOS-86916	Major	Unable to sign zones that have Unicode characters in the IDN names.
NIOS-85622	Major	Under certain circumstances, extensible attribute topology database rebuild failed.

ID	Severity	Summary
NIOS-88304	Minor	Unable to click the center part of the “+” button to add nameservers to a zone.

Issues Fixed in NIOS 8.6.2.2 Consolidated Hotfix-2

ID	Severity	Summary
NIOS-88280	Major	NIOS was vulnerable to CVE-2022-3488.

Issues Fixed in NIOS 8.6.2.1 Consolidated Hotfix-1

ID	Severity	Summary
NIOS-85707	Critical	Under certain circumstances, Amazon Route 53 synchronization tasks took a long time to complete.
ID	**Severity**	**Summary**
NIOS-88141	Major	DNS administrators were unable to modify TXT records and the “Access Denied: Only superusers can read admin groups.” error message was displayed in Grid Manager.
NIOS-87822	Major	After a NIOS upgrade, unable to modify or create networks, zones, and extensible attributes and the “The database is locked by background tasks. Operation is not permitted.” error message was displayed.
NIOS-87456	Major	NIOS was vulnerable to CVE-2022-2928 and CVE-2022-2929.
NIOS-87226	Major	NIOS was vulnerable to CVE-2022-38177, CVE-2022-38178, and CVE-2022-2795.
NIOS-86947	Major	Under certain circumstances, the DNS service stopped responding to authoritative and recursive DNS queries.
NIOS-86932	Major	Under certain circumstances, Amazon Route 53 synchronization tasks took a long time to complete.
NIOS-86278	Major	The SFP ports on the TE-4005 appliance were labeled incorrectly and were in reverse order of the label.
NIOS-86190	Major	Threat Insight did not add exfiltration domains to the blacklist when using the DEX tool.

NIOS-85837	Major	Under certain circumstances, unable to delete nameserver groups and the following error message was displayed in Grid Manager: An error has occurred. Contact technical support if the problem persists.
NIOS-85360	Major	When the DNS Traffic Control server and the DNS Traffic Control pool were disabled without configuring a health monitor, partial health update requests failed.
NIOS-84665	Major	The DNSKEY record for a KSK (Key Signing Key) was automatically deleted for multiple zones.
NIOS-83155	Major	An HA Grid Master that was serving a DHCPv6 server started discarding renew requests after an HA failover due to changes in DUID.
NIOS-81730	Major	NIOS was vulnerable to CVE-2021-20322.

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