Vulnerabilities in Nozomi Guardian/CMC

Overview

Nozomi disclosed multiple vulnerabilities in their Guardian/CMC product on August 9th, 2023, and has issued patches to address these issues.

Affected Products and Versions

Nozomi Guardian/CMC

- All versions prior to v22.6.2

Authenticated Blind SQL Injection on Sorting (CVSS Score: 7.1)

A blind SQL Injection vulnerability in Nozomi Networks Guardian and CMC, due to improper input validation in the sorting parameter, allows an authenticated attacker to execute arbitrary SQL queries on the DBMS used by the web application.

Authenticated Blind SQL Injection on Alerts Count (CVSS Score: 7.1)

A blind SQL Injection vulnerability in Nozomi Networks Guardian and CMC, due to improper input validation in the alerts_count component, allows an authenticated attacker to execute arbitrary SQL queries on the DBMS used by the web application.

Stored Cross-Site Scripting in Threat Intelligence Rules (CVSS Score: 6.4)

An authenticated attacker with administrative access to the appliance can inject malicious JavaScript code inside the definition of a Threat Intelligence rule, that will later be executed by another legitimate user viewing the details of such a rule.

Information Disclosure via the Debug Function in Assertions (CVSS Score: 6.5)

An access control vulnerability was found, due to the restrictions that are applied on actual assertions not being enforced in their debug functionality.

Partial DoS on Reports Section due to Null Report Name (CVSS Score: 4.3)

A partial DoS vulnerability has been detected in the Reports section, exploitable by a malicious authenticated user forcing a report to be saved with its name set as null.

DoS via SAML Configuration (CVSS Score: 4.9)

An authenticated administrator can upload a SAML configuration file with the wrong format, with the application not checking the correct file format. Every subsequent application request will return an error.

Session Fixation (CVSS Score: 5.0)

In certain conditions, depending on timing and the usage of the Chrome web browser, Guardian/CMC versions before 22.6.2 do not always completely invalidate the user session upon logout. Thus an authenticated local attacker may gain access to the original user's session.

Exploitation Status

GE Gas Power Product Security has not observed nor received reports of any exploit attempts against Gas Power Customers.

Remediation/Mitigation

GE Gas Power has performed validation of recent Nozomi releases and approved installation of v22.6.3 in customer environments, which will address all the above vulnerabilities.

It is recommended to back up your configuration prior to performing the update – below is the process for backing up your device's configuration:

Web UI

To perform a backup from the Web UI, go to **Administration** > **System** > **Backup/Restore**.

You can perform the following functions from the **Backup/Restore** screen:

- **Generate Backup Archive** (click the **Download** button)
- **Restore Previous Backup** (select a previous backup to restore and upload the file)
- **Schedule Backup Archive generation** (schedule a backup for a chosen date or recurrence by clicking the **Schedule backup** button)

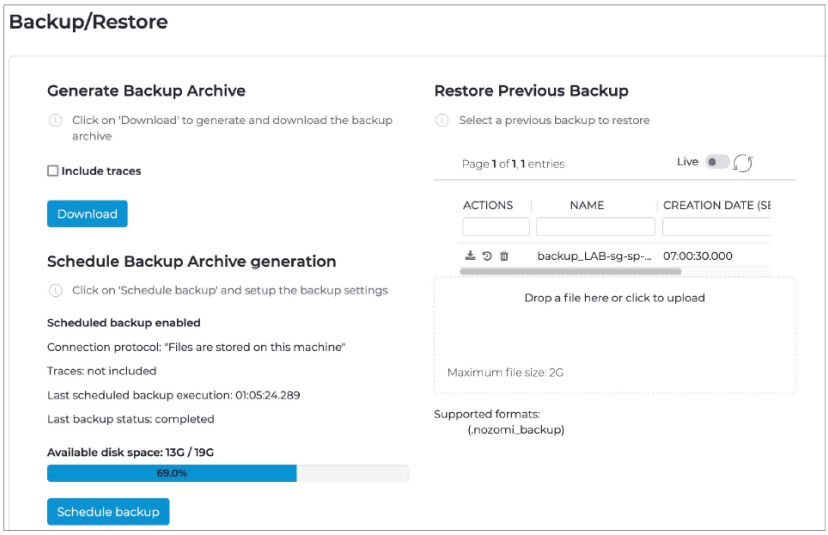


Figure 207: Backup/restore

When scheduling a backup, you can configure the frequency of recurrences, the maximum number of backups to retain, and the location to store backup files. Locations can be either local or remote.

- If local, backup files are stored in the `/data/backups/` folder on the appliance.
- If remote, backup files are stored on a dedicated host. This host provides a user/password authentication method using a listed protocol. The user must have folder permission to list, read, and write to store the backup files. During the backup process, the backup file generates locally and then uploads to the remote folder. When restored, the backup file first downloads from the remote folder and is then used in the restore process.

After backing up your configuration, you may perform the update to your system. Please note the update path listed below to ensure that any intermediary updates are installed as necessary:

Update Path Recommendation

If you are on a **19.x** release - version support has ended as of March 1st, 2022

- Please see update remarks of 20.0.0 (listed below for convenience).

If you are on a **20.x release older than 20.0.7.7**:

- 20.x > 20.0.7.7 > 21.9.0 > 22.6.3

A rollback from a version newer than 20.0.7.7 to 20.0.7.7 is not supported.

If you are on a **21.x older than 21.9.0**:

- 21.x > 21.9.0 > 22.6.3

If you are on the release **21.9.0 or newer**:

- Upgrade directly to 22.6.3

20.0.0 update remarks

- If upgrading from a version < 18.5.9 see update remarks of 19.0.0.
- Version 20.0.0 introduces SSH key based authentication and blocks SSH password login for the `root` user. SSH password login is allowed only when using the `admin` user. If you are upgrading from version 18.5.9 to version 20.0.0, or if you don't use the admin user yet, you'll need to add a SSH key using the WebGUI in order to be able to login. Refer to the user manual for more information about how to configure SSH keys.
- Ensure enough space is available in `/data` before update execution. As a rule of thumb check that the appliance has at least 15% of free disk space or at least 5GB free. To perform an exact check use the `n2os-db-stats` command to gather the database size and check that the free space on disk is bigger that the sum of all the tables. The update process can take a long time, depending on the amount of data and the complexity of the system, but it generally takes less than a few minutes.
- To update a Docker container edition a manual database dump is mandatory:

```
docker exec -d <CID> \
bash -c "pg_dump scadaguardian -U n2os-dbms | gzip -9 > /
data/dump-updatev"
```

Where <CID> is the container id of your current running container. After dump execution stop old container and start the new one.

Once you have validated your update path, the updates can be installed by following these instructions (you may opt either to install via the web UI or via command line interface):

1. Visit Nozomi Customer Portal. Create an account if you don't already have one.
2. After creating the account is created successfully, you can login to the support portal. Click on 'Product Releases'.
3. Then click on the 'Release Package' link you want to download. At the next page under 'Update Bundles' click on the 'Update Package' link to download the update bundle file.
4. Follow instructions given below to update Nozomi appliances.

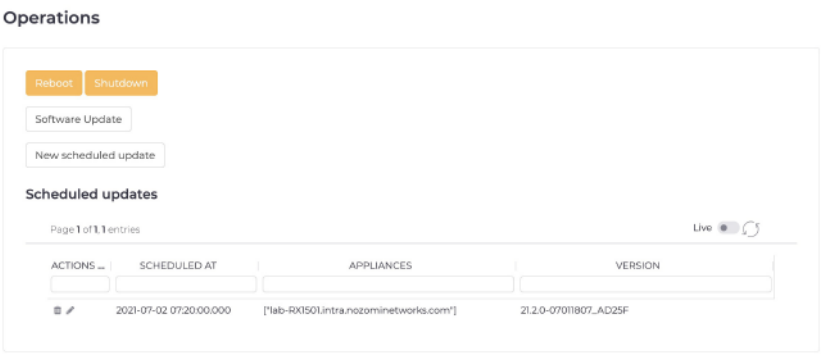
Update: from Web UI

This topic describes how to update the Nozomi Networks solution software in an existing installation.

You must have the new *VERSION-update.bundle* file that you want to install.

A running system is updated with a more recent N2OS release, as follows:

1. From the Web UI, go to **Administration** > **System** > **Operations**.



2. Click **Software Update** and select the *VERSION-update.bundle* file.

   Note: The system must be at least version 18.5.9 to support the *.bundle* format. If your system is running a version lower than 18.5.9 you must first update to 18.5.9 to proceed.

   The file is uploaded.
3. Click the **Proceed** button.

   Note: If updating from version 18.5.9, the system prompts you to insert the checksum that is distributed with the *.bundle*; the button is enabled only after checksum is verified.

   The update process begins. The update may take several minutes to complete.

Update: from CLI

This topic describes how to update the Nozomi Networks solution software in an existing installation.

You must have the new *VERSION-update.bundle* file that you want to install.

A running system is updated with a more recent N2OS release, as follows:

1. From a shell console, type `cd` to navigate to the directory where the *VERSION-update.bundle* file is located.
2. Copy the *VERSION-update.bundle* file to the appliance using the following command:

```
scp VERSION-update.bundle admin@<appliance_ip>:/data/tmp
```

   Note: The system must be at least version 18.5.9 to support the *.bundle* format. If your system is running a version lower than 18.5.9 you must first update to 18.5.9 to proceed.

   The file is uploaded.
3. Start the installation of the new software with the following commands:

```
ssh admin@<appliance_ip>
```

```
enable-me
```

```
install_update /data/tmp/VERSION-update.bundle
```

Resources

https://security.nozominetworks.com/

Contact Information

Contact your local GE Services representative for assistance or for additional information.
For Product Security issues or incident/vulnerability reporting: www.ge.com/power/cybersecurity

Document History

Version	Release Date	Purpose
1.0	9/19/2023	Initial Release