Mandiant

APPLY SECURITY UPDATES TO SECURITY VALIDATION APPLIANCES

The operating system that is used by Security Validation appliances (OVA-, VHD-, or AMI-based Directors, Actors, and Protected Theater) requires updates to address vulnerabilities that are found in OS components.

You can apply updates using the following methods:

- Automatic security updates: Mandiant recommends that you enable automatic security updates. This way, your environment receives the latest security updates as soon as they're available. How you enable automatic updates depends on the version of Mandiant Security Validation (MSV) that you're running in your environment.
- Manual security updates: You can choose the manual option, if needed. This method is also required to receive the latest Mandiant SecOps Integrations (MSI) releases.

Automatic

Instead of applying security updates released by the Security Validation team, you can enable automatic updates on a Director, Actor, or Protected Theater appliance.

Choose the section that is relevant to your MSV release:

- **4.14.0.0 and later**
- **4.13.0.0 and earlier**

4.14.0.0 and later appliances

Mandiant Security Validation (MSV) 4.14.0.0 onward uses Rocky Linux 8.x as the underlying operating system. This operating system is preconfigured to fetch and apply updates automatically. No manual steps are required to set this up.

Mandiant SecOps Integrations (MSI) releases are released through security updates. However, MSI service updates are only included in manually-applied updates. Therefore, to obtain the latest MSI release, you must manually download the latest security update and then apply it by using the **Apply security updates to appliances using the web interface** method.

If you have to add destinations of outbound connections to an allowlist, the system connects to any mirror on the Rocky Linux 8.x mirror lists for Rocky Linux-based appliances.

4.13.0.0 and earlier appliances

If you have an internal CentOS 7 /EPEL yum mirror, you can use that mirror; however, the following instructions are for the default public mirrors.

If you have to add destinations of outbound connections to an allowlist, the system connects to any mirror on the CentOS 7 or Fedora EPEL mirror lists.

Enable automatic security updates (4.13.0.0 and earlier)

1. Disable the `verodin.repo` file:

```
sudo sed -i -e 's/enabled=1/enabled=0/g' /etc/yum.repos.d/verodin.repo
```

2. Install yum-cron:

```
sudo yum install yum-cron -y
```

3. Edit `/etc/yum/yum-cron.conf` to enable the updates to apply automatically:

- Change `apply_updates = no` to `apply_updates = yes`

```
sudo sed -i -e 's/apply_updates = no/apply_updates = yes/g' /etc/yum/yum-cron.conf
```

4. Enable yum-cron:

```
sudo systemctl enable yum-cron
```

5. Start yum-cron:

```
sudo systemctl start yum-cron
```

Within the next 24 hours to a week, you start to see activity in `/var/log/yum.log`, which signifies that packages are being updated. You can run the following command to show the most recent lines in that log file:

```
sudo tail -f /var/log/yum.log
```

- If you have automatic security updates enabled through `yum-cron` and need to update to the latest version of the integrations service without performing a full system update, apply the most recent security update manually. Integration service updates are only included in manually-applied security updates and system updates.
- Regarding yum security and why it can be trusted, yum uses information, which includes a centralized, non-mirrored Fedora-run metalink service. This service provides a list of active mirrors and the cryptographic digest of the `repomd.xml` files, which yum uses to select a mirror and to verify that it serves the up-to-date `repomd.xml`. The chain of cryptographic digests is then verified, which leads to the verification of the `.rpm` file contents.

Recreate the verodin.repo file (4.13.0.0 and earlier)

If you delete the `verodin.repo` file, you can recreate it by running the following commands:

Director

```
$ sudo su -
# cd /etc/yum.repos.d
# echo -e "[verodin]\nname=Verodin CentOS Repo\nbaseurl=file:///opt/apps/verodin/planner/tmp/verodin_repo/centos
\ngpgcheck=0\nenabled=0" > verodin.repo
```

Actor

```
$ sudo su -
# cd /etc/yum.repos.d
# echo -e "[verodin]\nname=Verodin CentOS Repo\nbaseurl=file:///opt/apps/verodin/node/tmp/verodin_repo/centos\n
gpgcheck=0\nenabled=0" > verodin.repo
```

Configure yum for proxy access (4.13.0.0 and earlier)

Some customers might need to use a proxy to access yum. Use the following steps to update the `yum.conf` file for any hosts that are self-updating through a proxy.

These steps are recommended only for power users or support personnel. Proxy issues are difficult to debug by anyone that didn't set up the proxy. If the customer runs into issues, then the product administrator must debug with the network administrator before engaging Mandiant for support. The debug details are most likely at the proxy level and not in the product.

1. Connect to the Director or Actor through SSH.
2. Switch to an elevated command prompt:

```
sudo bash
```

3. Open the yum config file:

```
vi /etc/yum.conf
```

4. Add the following lines to the end of the file:

   If the proxy is not authenticated, then omit the last two entries.

```
[main]
 ...
proxy=<protocol>://<proxy ip>:<proxy port>
proxy_username=<username>
proxy_password=<password>
```

   For example, if the proxy uses HTTPS protocol, IP address 203.0.113.1, port 9876, and the username is `exampleuser` with a password of `examplepassword`, then the configuration file update looks like the following:

```
[main]
 ...
proxy=https://203.0.113.1:9876
proxy_username=exampleuser
proxy_password=examplepassword
```

5. Save your changes: press `Esc`, type `:w`, and then press `Enter`.

Manual

Use a preferred method to manually install security updates:

- **Director web interface**
- **Command line interface**

Manually apply security updates to appliances using the web interface

Before you begin, keep the following in mind:

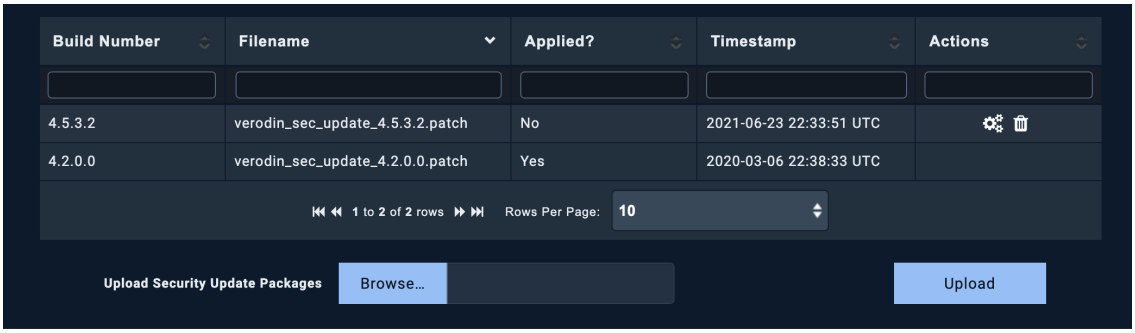
- Always install the latest update that's listed on the Security Updates page.
- If your Actor acts as a proxy for another Actor, your Actor must have a minimum of 8 GB storage before applying the security update.
- If you used a Validation installer to install the Director or Actor on an operating system you maintain (for example, Windows, macOS, or Linux), the security updates won't work for you; they only work on appliances.

1. Download the update file from the **Security Update Downloads page (https://docs.mandiant.com/home/msv-security-update-downloads)**.

> Security package naming format: `verodin_sec_update_rocky8_VERSION.patch`, where *VERSION* is the version string in the filename.

2. In the Director web interface, go to **Settings > Director Settings**. On the System Settings page, in the **Upload Security Update Packages** field, navigate to the package and upload the file.
3. Upload the update to the Director. When the upload completes, your System Updates page refreshes and looks similar to the following image. If you have an appliance-based Director, it includes a **Stage** icon.

> This step is required to upload security updates for the Actor and Protected Theater, even if you don't have an appliance-based Director.



Security update info

4. If necessary, apply the update to your Director.
   a. Click **Stage**. A message displays asking you to confirm that the hash values match the update that you want to apply. If the hash value is correct, click **OK**.
   b. Click **Reboot** (`vrestart` does not trigger the install).
5. Apply the update to the appliance-based Actors and Protected Theaters.
   a. Look at the Actor Versions section of the System Updates page to identify which Actors are installable software and which are appliances.

> - If you see **Package** next to the Actor name, the Actor is installable software and not an appliance.
> - If you see a **Run Security Updates** button, the Actor is an appliance.

   b. If available, click **Run Security Updates** to apply the security update.

Manually apply security updates using the command line

Follow the commands in these tasks to apply the security update to your Director or Actor. You must use an account with sudo or root privileges to run the security update this way.

> If you use this method, you are not required to update the Director before updating your Actors or Protected Theater.

Director

1. On the system where you downloaded the file, run the following command:

```
$ scp verodin_repo_x.x.x.x.tar.gz nodeone@<DIRECTOR_IP>:
```

Where *x.x.x.x* refers to the version number of the downloaded file and *DIRECTOR_IP* is the IP address of the Director that you want to connect to.

2. On the Director, run the following commands one-by-one to install the update and reboot to apply it:

```
$ sudo rm -fR /opt/apps/verodin/planner/tmp/verodin_repo
```

```
$ sudo tar xf verodin_repo_x.x.x.x.tar.gz -C /opt/apps/verodin/planner/tmp/
```

```
$ sudo yum clean all
```

```
$ sudo yum update --disablerepo="*" --enablerepo="verodin" -y
```

```
$ sudo rm -fR /opt/apps/verodin/planner/tmp/verodin_repo
```

```
$ sudo reboot
```

Actor and Protected Theater

On the system where you downloaded the file:

```
$ scp verodin_repo_x.x.x.x.tar.gz nodeone@ACTOR_IP:
```

Where *x.x.x.x* refers to the version number of the downloaded file and *ACTOR_IP* is the IP address of the Actor that you want to connect to.

On the Actor or Protected Theater, run the following commands one-by-one to install the update and reboot to apply it:

```
$ sudo rm -fR /opt/apps/verodin/node/ext/verodin_repo
```

```
$ sudo tar xf verodin_repo_x.x.x.x.tar.gz -C /opt/apps/verodin/node/ext/
```

```
$ sudo ln -s /opt/apps/verodin/node/ext/verodin_repo/centos /opt/apps/verodin/node/ext/verodin_repo/rocky8
```

```
$ sudo yum clean all
```

```
$ sudo yum update --disablerepo="*" --enablerepo="verodin" -y
```

```
$ sudo rm -fR /opt/apps/verodin/node/ext/verodin_repo
```

```
$ sudo reboot
```