Security Enhancements for Advanced Malware Detection

Advanced Malware Detection | v8.5.x | March 2020

Use the information provided in this document to enhance the security of your web protection solution. The details provided below allow you to harden your system and ensure you are using the best security measures available.

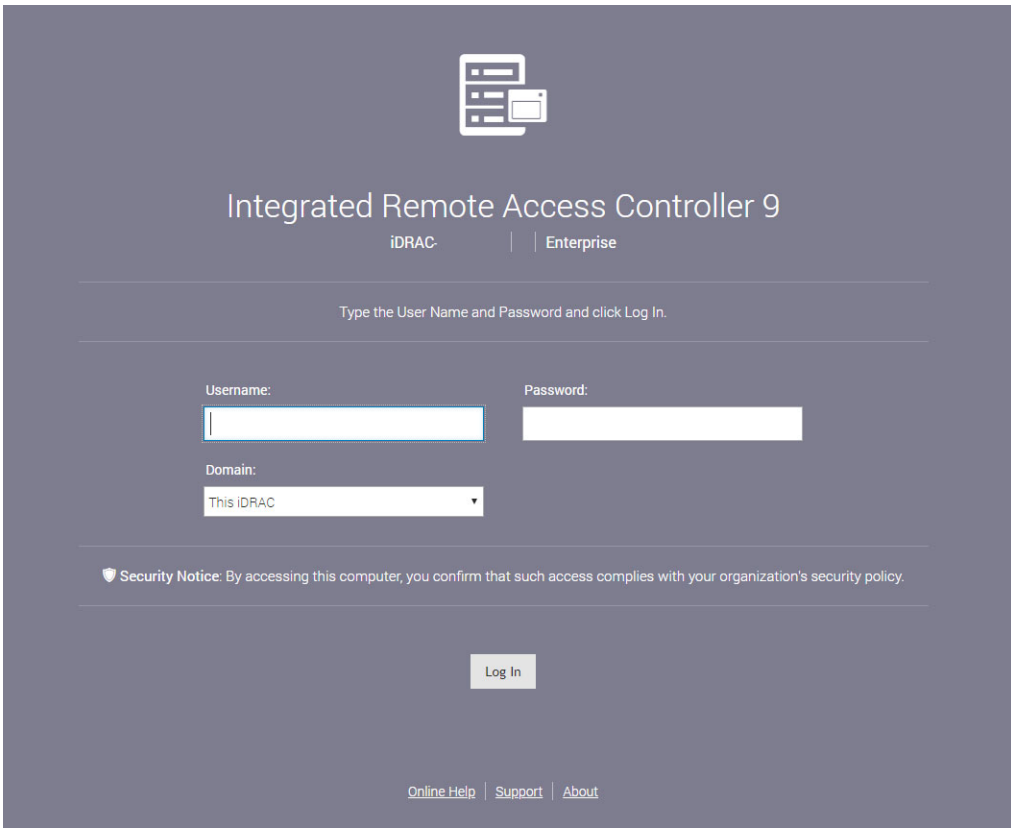
As a general recommendation, it is always best to install hotfixes as soon as they are available.

Prerequisites

Perform these security enhancement steps after the complete installation of the Forcepoint AMD-Manager Appliance and Forcepoint AMD Engine Appliance.

Since a there are a few activities requiring interaction with changing the operating kernel while the Appliance is booting up, it is necessary to run these steps through

Dell's iDRAC, HP's iLo, or IBM's LOM to complete these tasks in the native command line application.



Before continuing, please ensure that the user has root privileges so all items can be performed without complication.

Also, AMD-1.0 repo will need to be deactivated. To deactivate before performing any of the steps and to reactivate when complete, run the following commands.

- Disable the pre-configured repo with the following command:

  ```
  [root@amd-manager:~]# yum-config-manager --disable AMD-1.0
  ```

- Re-enable the pre-configured repo with the following command:

  ```
  [root@amd-manager:/home/admin]# yum-config-manager --enable
  AMD-1.0
  ```

Update kernel (highly recommended)

The Steps below will update a critical component that is used to operate the hardware that Forcepoint AMD Appliance uses.

1. Ensure that you have an outdated kernel. For most machines this package would be “3.10.0-327.el7”.

   ```
   [root@amd-manager:~]# uname -srm
   ```

2. Query repositories for available package updates.

```
# yum check-update
```

3. Install the latest mainline stable kernel.

   ```
   # yum install kernel
   ```

   a. When prompted to accept the total download size, type **Y** and press **Enter**.

   b. When prompted to accept the GPG key, type **Y** and press **Enter**.

4. Verify that the latest kernel package was installed (kernel-3.10.0-1062.9.1 or later).

   ```
   # rpm -qa | grep kernel
   ```

5. Reboot and verify that the kernel was properly installed. When the GRUB menu appears with a list of kernels, select the newly-installed kernel. If it is not automatically selected, it may be best to configure GRUB to automatically boot with the latest kernel.

6. Login as root, and run the following command.

   ```
   # uname -sr
   ```

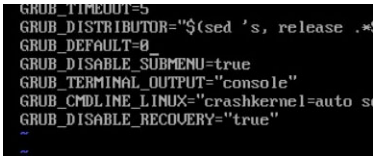
The following displays:

Change GRUB to boot with the newest kernel (recommended)

1. Configure GRUB to always boot with the new kernel.

   a. Open /etc/default/grub

   b. Set GRUB_DEFAULT=0



2. Recreate the kernel configuration.

   ```
   # grub2-mkconfig -o /boot/grub2/grub.cfg
   ```

3. Reboot and verify that the latest kernel is being used as the default.

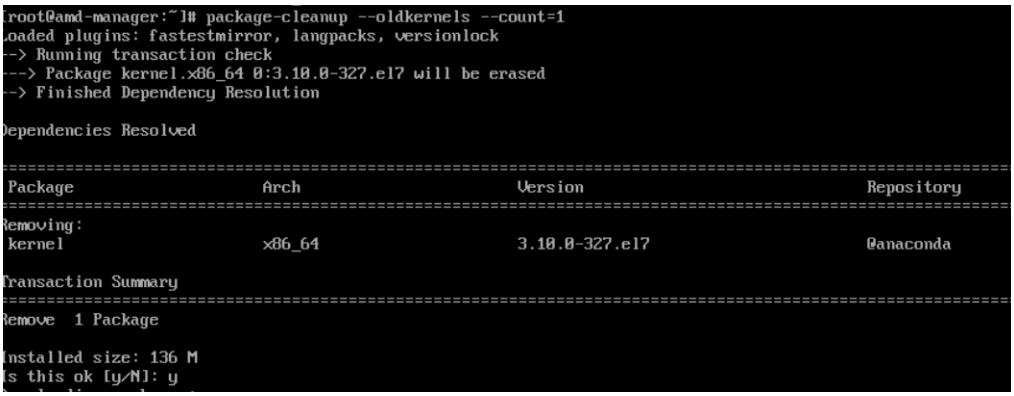
Remove the old kernel

This will reduce the risk of a user choosing or the system automatically rebooting into the old vulnerable kernel.

1. Remove the old unused kernel package. Verify that you are using the latest kernel (kernel-3.10.0.1062 or later). Use the following command to remove the old kernel package.

   ```
   # package-cleanup -oldkernels --count=1
   ```

2. When prompted to verify the removal of the kernel, 3.10.0-327.el7, press **Y**.



Update all of the installed packages from CentOS where an update is available (highly recommended)

The steps below will allow the Forcepoint AMD customer to update the packages that need both critical and non-critical updates from CentOS. This will ensure that the product is fully secure from all known vulnerabilities.

Enable YUM REPO

1. Update the list of available public repositories.

   ```
   [root@amd-manager:/home/admin]# yum -v repolist
   ```

2. Check for any available updates to the installed packages.

   ```
   [root@amd-manager:/home/admin]# yum check-update
   ```

3. Download updates for the installed packages.

   a. When prompted with Is this ok [y/d/N], press D for download.

   ```
   [root@amd-manager:/home/admin]# yum --exclude=kernel\* update
   Transaction Summary
   ================================================
   Install   13 Packages (+150 Dependent packages)
   Upgrade  632 Packages
   Total size: 648 M
   Total download size: 645 M
   Is this ok [y/d/N]: d
   ```

4. Update the installed packages with the packages downloaded in step 3.

a. When prompted with Is this ok [y/d/N], press Y.

```
[root@amd-manager:/home/admin]# yum -exclude=kernel\*
update
Transaction Summary
=====================================================
Install   13 Packages (+150 Dependent packages)
Upgrade  632 Packages
Total size: 648 M
Is this ok [y/d/N]: Y
Downloading packages:
warning: /var/cache/yum/x86_64/7/base/packages/libdb-
5.3.21-25.el7.i686.rpm: Header V3 RSA/SHA256 Signature,
key ID f4a80eb5: NOKEY
```

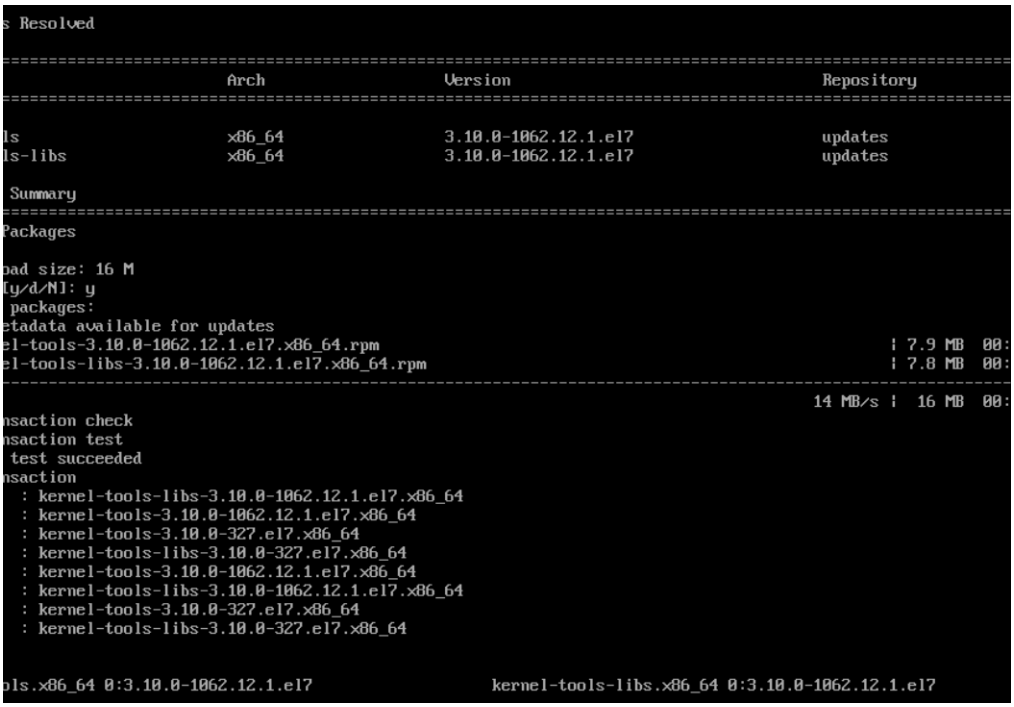
b. When prompted to accept the GPG Key, press Y to accept the GPG Key.

```
Retrieving key from file:///etc/pki/rpm-gpg/RPM-GPG-KEY-
CentOS-7
Importing GPG key 0xF4A80EB5:
Userid     : "CentOS-7 Key (CentOS 7 Official Signing Key)
<security@centos.org>"
Fingerprint: 6341 ab27 53d7 8a78 a7c2 7bb1 24c6 a8a7 f4a8
0eb5
               Package    : centos-release-7-
2.1511.el7.centos.2.10.x86_64 (@anaconda)
               From       : /etc/pki/rpm-gpg/RPM-GPG-KEY-
CentOS-7
Is this ok [y/N]: y
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction
```

5. Verify that no other updates are required (kernel-tools for kernel 3.10.0-327 will need to be removed). Running yum update once more will ensure you have the latest kernel-tools 3.10.0-1062 and remove the old unused kernel-tools.

```
# yum update
```

- Press 'y' when confirming this transaction, as seeing below.



6. Reboot the computer to complete the package updates.

Update Nginx version to 1.16 or newer (highly recommended)

When you perform a “yum update Nginx”, the default CentOS repository does not always come back with the latest updates. These steps will add an additional repository with the latest Nginx updates that will mitigate most of latest issues.

1. Create a new repository file with the following command.

   ```
   # vi /etc/yum.repos.d/nginx.repo
   ```

2. Add the following repo definition into the file and save the file.

   ```
   [nginx]
   name=nginx repo
   baseurl=http://nginx.org/packages/centos/$releasever/
   $basearch/
   gpgcheck=0
   enabled=1
   ```

3. Stop Nginx by running the following command.

   ```
   # systemctl stop nginx
   ```

4. Update Nginx.

   ```
   # yum update nginx
   ```

5. Start Nginx, and Nginx update should be complete.

Update Nginx to the latest secure practices

It is highly recommended that Nginx is configured to the latest security practices. You will need to have performed the Nginx update above to continue, as the current Nginx version does not support TLSv1.3. To make the following changes, open /etc/Nginx / nginx.conf.

1. Turn server tokens off.

   Disabling server tokens makes it more difficult to determine the Nginx version, and therefore more difficult for an attacker to execute version-specific attacks.

   Within the Nginx .conf file, find configuration for http. Within the http brackets ('http{…}'), add the following line.

   ```
   'server_tokens off;'
   ```

2. Disable TLSv1.0 and TLSv1.1 within Nginx.
   a. Within 'http{…}', find configuration for ssl_protocols. The protocols maybe listed as:

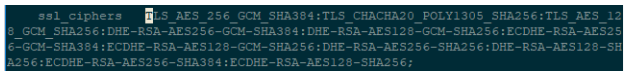
      ```
      ssl_protocols       TLSv1 TLSv1.1 TLSv1.2;
      ```

   b. Ensure that the Nginx is the latest stable version. Remove TLSv1 and TLSv1.1 and add TLSv1.3. The following line should look like this.

      ```
      ssl_protocols       TLSv1.2 TLSv1.3;
      ```

3. Configure the recommended owasp ciphers for Broad Capability (B). (See the owasp cheat sheet for details: https://cheatsheetseries.owasp.org/cheatsheets/TLS_Cipher_String_Cheat_Sheet.html)
   a. Within the 'http{…}' configuration group modify the list of 'ssl_ciphers' to have the following list:

      ```
      TLS_AES_256_GCM_SHA384:TLS_CHACHA20_POLY1305_SHA256:TL
      S_AES_128_GCM_SHA256:DHE-RSA-AES256-GCM-SHA384:DHE-
      RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-
      SHA384:ECDHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES256-
      SHA256:DHE-RSA-AES128-SHA256:ECDHE-RSA-AES256-
      SHA384:ECDHE-RSA-AES128-SHA256;
      ```

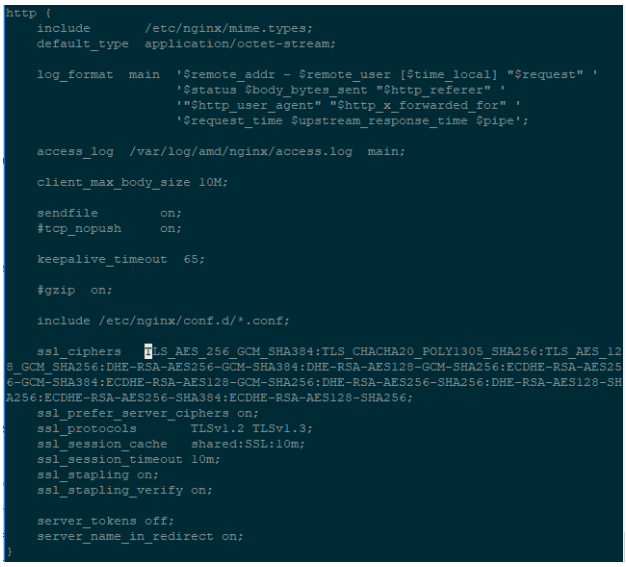
   b. This list should replace the following list:

      ```
      EECDH+AESGCM:EDH+AESGCM:AES256+EECDH:AES256+EDH;
      ```

> **Note**
> Do not forget the semi-colon at the end of the line.

4. There is a known vulnerability that discloses the IP address of the appliance when using the expected FQDN (See CVE-2000-0649). To resolve this issue, within the 'http{…}', add the following line.

   ```
   server_name_in_redirect on;
   ```



5. Finish by saving the Nginx .conf file and restarting Nginx with the following commands.

   ```
   # nginx  -s reload
   # systemctl restart nginx
   ```

Disable redirect: access the appliance through HTTPS only

Deactivating port 80 is the recommended option to force users to directly work with port 443 instead of being redirected from port 80 to the more secure port 443. While being redirected, the IP address is openly shared.

1. Logon on as root user and open shim_ng.conf.

   ```
   # vi /etc/nginx/conf.d/shim_ng.conf
   ```

2. Add '#' in front of 'listen 80;' and save the changes by typing the following ':wq'.

3. Restart Nginx for the changes to be accepted.

   ```
   # systemctl restart nginx
   ```

Secure SSH server side communication

Configure the following on the SSH Daemon to ensure a more secure line of communication via SSH.

Open and modify /etc/ssh/sshd_config by adding the following lines, preferably below the MACs or Ciphers line.

```
HostKeyAlgorithms ssh-rsa, rsa-sha2-512, rsa-sha2-256
```

and

```
KexAlgorithms curve25519-sha256, curve25519-
sha256@libssh.org, ecdh-sha2-nistp256, ecdh-sha2-
nistp384, ecdh-sha2-nistp521, diffie-hellmangroup-
exchange-sha256, diffie-hellman-group16-sha512,
diffiehellman-group18-sha512, diffie-hellman-group-
exchange-sha1, diffiehellman-group14-sha256, diffie-
hellman-group14-sha1, diffie-hellmangroup1-sha1
```

These lines prompt any SSH client to use the following algorithms when attempting to connect to AMD through SSH.

Change the web server SSL certificate

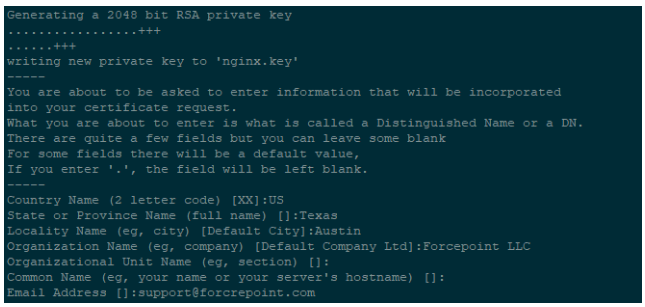
Certificate requirements are:

- The certificate must be in x509 Format.
- The generated certificate must not have a pass-phrase.

Perform the following steps to change your certificate:

1. Change your working directory to the following folder: '/usr/local/amd/shim/conf/Nginx /ssl/'.
2. In this directory, save a copy of both Nginx .crt and Nginx .key. (Example: Save 'Nginx .crt' as 'Nginx .crt.old')
3. In the same directory, generate the following certificate with the following command:

   ```
   # openssl req -x509 -sha256 -nodes -days <days> -newkey
   rsa:2048 -keyout nginx .key -out nginx .crt
   ```

4. Restart Nginx with the following command.

```
# systemctl restart nginx
```