Aurora, WebMail, MailSuite

Web-based solutions from AfterLogic

Addressing DAV-related vulnerability in WebMail and Aurora

FEBRUARY 3, 2021MARCH 25, 2021

One of our valued customers reported a vulnerability in our products, that potentially allows uploading and executing arbitrary files via built-in DAV server used in WebMail Pro (https://afterlogic.com/webmail-client) and Aurora Corporate (https://afterlogic.com/aurora). We're now releasing updates for our products closing this vulnerability, and strongly recommend to upgrade your installations to the latest version.

Below, you'll find recommendations on how to address the issue on your existing installation of WebMail Pro or Aurora. Please note that while these changes were only tested with version 8.5.3, they should work for previous versions as well.

Before we proceed, we'd like to point out that disabling DAV access on the installation effectively closes the vulnerability, too. That's done by setting **Disabled** to **true** in data/settings/modules/Dav.config.json file. Note that this will not affect the use of web interface or Aurora Mail / Aurora Files mobile apps as they work via API, not DAV. If you'd rather keep DAV enabled, please follow the below guidelines.

1. In vendor/afterlogic/dav/lib/DAVServer.php file, locate function **exec**() and replace its code with:

```
public function exec()
{
    $sRequestUri = empty($_SERVER['REQUEST_URI']) ? '' : \trim($_SERVER['REQUEST_URI']);

    if ($this->isModuleEnabled('Dav') && !strpos(urldecode($sRequestUri), '../'))
    {
        parent::exec();
    }
    else
    {
        echo 'Access denied';
    }
}
```

2. In vendor/afterlogic/dav/lib/DAV/Auth/Backend/Basic.php file, locate **validateUserPass** function and replace the line:

```
if (class_exists('\\Aurora\\System\\Api') && \Aurora\System\Api::IsValid())
```

with:

```
if (class_exists('\\Aurora\\System\\Api') && \Aurora\System\Api::IsValid() && $sUserName !== \Afterlogic\DAV\Constants::DAV_PUBLIC_PRINCIPAL && $sUserName !== \Aft
```

3. Similarly, in vendor/afterlogic/dav/lib/DAV/Auth/Backend/Digest.php file, locate **getDigestHash** function and replace the line:

```
if (class_exists('\\Aurora\\System\\Api') && \Aurora\System\Api::IsValid())
```

with:

```
if (class_exists('\\Aurora\\System\\Api') && \Aurora\System\Api::IsValid() && $sUserName !== \Afterlogic\DAV\Constants::DAV_PUBLIC_PRINCIPAL && $sUserName !== \Aft
```

Since some of our clients still use previous v7 of WebMail and Aurora, we chose to issue a security update for those as well. Note that if you don't use DAV, you can simply disable it by setting **EnableMobileSync** to **Off** in data/settings/settings.xml file.

1. In libraries/afterlogic/DAV/Server.php file, before the closing "}" add the following function:

```
public function exec()
{
    $sRequestUri = empty($_SERVER['REQUEST_URI']) ? '' : \trim($_SERVER['REQUEST_URI']);
    if (!strpos(urldecode($sRequestUri), '../'))
    {
        parent::exec();
    }
    else
    {
        echo 'Access denied';
    }
}
```

2. In libraries/afterlogic/DAV/Auth/Backend/Basic.php file, locate **validateUserPass** function and replace the line:

```
if (class_exists('CApi') && \CApi::IsValid())
```

with:

```
if (class_exists('CApi') && \CApi::IsValid() && $sUserName !== \afterlogic\DAV\Constants::DAV_PUBLIC_PRINCIPAL && $sUserName !== \afterlogic\DAV\Constants::DAV_TEN
```

3. Similarly, in libraries/afterlogic/DAV/Auth/Backend/Digest.php file, locate **getDigestHash** function and replace the line:

```
if (class_exists('CApi') && \CApi::IsValid())
```

with:

```
if (class_exists('CApi') && \CApi::IsValid() && $sUserName !== \afterlogic\DAV\Constants::DAV_PUBLIC_PRINCIPAL && $sUserName !== \afterlogic\DAV\Constants::DAV_TEN
```

Should you require any assistance, please don’t hesitate to contact us (https://s.afterlogic.com/helpdesk/).