Security Configurations

The following security enhancements were added to prevent software vulnerabilities in all the OMK Applications.

Versions affected:

- opCharts 4.2.5
- opConfig 4.2.4
- opEvents 4.0.2
- opHA 3.3.1
- opReports 4.2.2

Randomize Secrets

A new tool to randomize the secrets from the command line. This tool will randomize *omkd_secrets* tokens in OMK and also, NMIS *auth_web_key* when it matches some of the OMK tokens. The *omkd_secrets* token is used for Single-Sign-On, see SSO for Opmantek Applications.

This tool is also called by the installer and fixed CVE-2021-38551.

Usage instructions:

```
/usr/local/omk/bin/opcommon-cli.exe act=secrets_randomise [force=true] [length=N]
```

Where:

- `force=true` will change the token even if this is not the default (Like =~ change_me)
- `length=N` will force the token length to N (32 by default)

Cookies

Cookie	Support	Behaviour
HttpOnly	✅ By default	The cookies are not going to be accessible from the JavaScript API.
secure	✅ Should be enabled by setting the configuration item "*auth_secure_cookie*" => "true" in opCommon.json.	This cookie could be sent just in a request ciphered over **https** protocol. That's the reason why it is not set by default.
SameSite set to *Strict*	✅ Supported since the following versions: • Open-AudIT 4.4.0 • opAddress 2.1.0 • opCharts 4.3.0 • opConfig 4.3.0 • opEvents 4.1.0 • opHA 3.4 • opReports 4.3.0	The cookie set to strict means that the browser only sends the cookie if the request was made in the website that originally established the cookie.

Content Security Policy

Content Security Policy is a HTTP response header that helps you restrict which resources (JavaScript, CSS, Images, etc.) are loaded from the allowed sites. This helps to mitigate some attacks of Cross Site Scripting (XSS) and data injection.

Some background information can be found here: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Content-Security-Policy

The default values can be overwritten by setting the configuration item **security_content_policy** under the authentication section in the configuration file, opCommon.json.

The default values included in the source code are:

```
"connect-src 'self' opmantek.com community.opmantek.com services.opmantek.com maps.googleapis.com ws: wss: maps.google.com maps.gstatic.com; font-src 'self' fonts.gstatic.com; form-action 'self'; frame-ancestors 'none'; frame-src 'none'; manifest-src 'none'; media-src 'none'; object-src 'none'; prefetch-src 'self'; script-src 'self' 'unsafe-eval' 'unsafe-inline' maps.googleapis.com maps.google.com; style-src 'self' fonts.googleapis.com 'unsafe-inline'; worker-src 'self';"
```

NOTE - Open-AudIT has slightly different default attributes - it includes the img-src tag, as well as adding maps.googleapis.com to the connect-src tag. See below.

```
"connect-src 'self' opmantek.com community.opmantek.com services.opmantek.com maps.googleapis.com ws: wss: maps.
google.com maps.gstatic.com; font-src 'self' fonts.gstatic.com; form-action 'self'; frame-ancestors 'none';
frame-src 'none'; img-src 'self' data: maps.google.com maps.gstatic.com; manifest-src 'none'; media-src 'none';
object-src 'none'; prefetch-src 'self'; script-src 'self' 'unsafe-eval' 'unsafe-inline' maps.googleapis.com
maps.google.com; style-src 'self' fonts.googleapis.com 'unsafe-inline'; worker-src 'self';"
```

Depending on what you need to achieve, you will need to update your configuration to include some or all of the default options as well as options specific to your environment.

For example, if you want to include one of the FirstWave applications in an iFrame, you would need to include directives for frame-ancestors and frame-src, e.g.

```
frame-ancestors https://*.yourdomain.com
frame-src https://*.yourdomain.com
```

The final configuration would be something like the following:

The below is formatted for easy reading. In the JSON file no line breaks should be used.

Note that you should replace *.yourdomain.com with an appropriate domain for your use-case.

```
"security_content_policy": "connect-src 'self' opmantek.com community.opmantek.com services.opmantek.com maps.
googleapis.com ws: wss: maps.google.com maps.gstatic.com;
    font-src 'self' fonts.gstatic.com;
    form-action 'self';
    frame-ancestors https://*.yourdomain.com;
    frame-src https://*.yourdomain.com;
    manifest-src 'none';
    media-src 'none';
    object-src 'none';
    prefetch-src 'self';
    script-src 'self' 'unsafe-eval' 'unsafe-inline' maps.googleapis.com maps.google.com;
    style-src 'self' fonts.googleapis.com 'unsafe-inline';
    worker-src 'self';"
```