

# CVE-2022-1096 - Delft-FEWS and Chromium (JCEF) vulnerability

Updated: April 15th 2022

## Statement:

On March 23, 2022, Google was alerted about a dangerous zero-day vulnerability found in all Chromium based browsers. An anonymous sender discovered the vulnerability, which is being tracked as CVE-2022-1096. The bug is a [type confusion vulnerability](#) and is currently being exploited by threat actors in the wild – making all Chromium based browsers vulnerable to attacks. The threat level for CVE-2022-1096 is rated “high” by Google. The vulnerability is a type confusion weakness located in the Chrome V8 JavaScript and WebAssembly engine. This flaw allows threat actors to execute arbitrary code on victim devices and allows the threat actor to trick Chrome into running malicious code. V8 is a component within Chrome that processes JavaScript, which is the engine that’s at the heart of Chrome.

## Impact on: Delft-FEWS Embedded Webbrowser (JCEF)

### Embedded Webbrowser: Impact is medium

The Delft-FEWS Embedded Web Browser is only used when configured in your application. If your Delft-FEWS application does not make use of the Embedded Web Browser then your application is not at risk. The Embedded Web Browser is used in your client application (Operator Client or Stand Alone).

### Detailed analysis:

The implementation of the Chromium Web Browser in Delft-FEWS has an extra security layer in the form of a “White List” so that only web domains that have explicitly been configured in the WebBrowserDisplay.xml configuration can be accessed within FEWS. This gives some extra protection, but in the event that one of the “white-listed” web sites is compromised this security leak in the Web Browser is a risk .

Friday 8th of April an update for the JCEF (Java Chromium Embedded Framework) became available and has been implemented in all supported FEWS branches that use Chromium and JCEF for the Web Browser display.

### Mitigation:

It is necessary to update your JCEF module that you can download from the [Web Browser wiki page](#) and install the latest patch (which includes an updated jcef.jar file) that can be requested through the FEWS helpdesk.

Delft-FEWS Product Management