



Wayne Kubick
HL7 CTO
Health Level Seven International
3300 Washtenaw Avenue, Suite 227
Ann Arbor, MI 48104

October 16, 2020

Dear HL7 Member,

The CDA Management Group has asked me to inform you of an important technical correction to XSLT Stylesheets that had been bundled with various implementation guides for the HL7® Clinical Document Architecture (CDA®) standard.

A security issue in version 4.0.0 of the generic stylesheet for display, which was originally released in May 2018, was recently identified by the CDA Examples Task Force. The security settings were allowing embedded content such as images of pdf files to be rendered in an iframe without an active sandbox, which could be vulnerable to the insertion of malicious content.

This issue has been corrected in a new version 4.0.2 beta 10 of the stylesheet. *Note that the sandbox attribute is not supported before Internet Explorer 9, so to avoid potentially unsafe contents in older versions of Internet Explorer, a switch has been added that entirely prevents iframes under these browser versions.*

An updated errata release has been created to remove the earlier version of the stylesheet from the download packages used to distribute CDA Implementation Guides. The updated download packages remove the vulnerable XSLT file and include a readme file with a link to the HL7 github repository where the updated version 4.0.2 beta 10 version that corrects the security vulnerability can be downloaded.

Alternatively, the corrected current stylesheet may be directly downloaded at <https://github.com/HL7/cda-core-xsl/releases/tag/v4.0.2-beta10>.

Users of versions 4.0.0 and 4.0.1 of the CDA stylesheet are strongly advised to upgrade to the latest version to mitigate this security risk.

Sincerely,

A handwritten signature in black ink, appearing to read "W. R. K.", with a long horizontal flourish extending to the right.

Wayne R. Kubick
HL7 CTO