



CVE-2014-5452

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

CVE	CVE-2014-5452
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-09-02 10:55:00 UTC
Updated	2016-12-22 02:59:00 UTC
Description	CDA.xml in HL7 C-CDA 1.1 and earlier does not anticipate the possibility of invalid C-CDA documents with crafted XML attri

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	HI7	C-cda	All	All	All	All

References

Reference

- HL7 C-CDA 'CDA.xml' Cross Site Scripting Vulnerability
- Security Bulletin: One vulnerability in IBM FileNet Content Manager and IBM Content Foundation (CVE-2013-5452)
- Security vulnerabilities in C-CDA Display using CDA.xml | SMART Platforms
- Healthcare Standards: HL7 CDA Stylesheet Patches
- HL7GForge > Projects > Structured Documents > Releases > Browse Frs Release
- IBM FileNet Content Manager XML External Entity Processing Flaw Lets Remote Users Obtain Potentially Sensitive Information - SecurityTrac
- CVE Program record
- NVD vulnerability detail

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)