



CVE-2014-3862

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

Summary

CVE	CVE-2014-3862
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-09-02 10:55:00 UTC
Updated	2014-09-02 19:04:00 UTC
Description	CDA.xsl in HL7 C-CDA 1.1 and earlier allows remote attackers to discover potentially sensitive URLs via a crafted reference

Risk And Classification

Problem Types: CWE-200

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference	Source	Link	Tags
Security vulnerabilities in C-CDA Display using CDA.xsl SMART Platforms	MISC	smartplatforms.org	Exploit
Healthcare Standards: HL7 CDA Stylesheet Patches	CONFIRM	motorcycleguy.blogspot.com	Patch
HL7GForge > Projects > Structured Documents > Releases > Browse Frs Release	CONFIRM	gforge.hl7.org	Patch
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, a

No vendor comments have been submitted for this CVE.

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

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