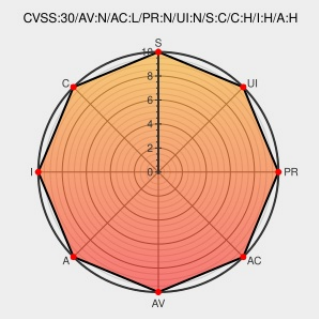
CVE-2015-8396

Published on: 01/12/2016 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:13 PM UTC

CVE-2015-8396

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Grassroots Dicom from Grassroots Dicom Project contain the following vulnerability:

Integer overflow in the ImageRegionReader::ReadIntoBuffer function in MediaStorageAndFileFormat/gdcmImageRegionReader.cxx in Grassroots DICOM (aka GDCM) before 2.6.2 allows attackers to execute arbitrary code via crafted header dimensions in a DICOM image file, which triggers a buffer overflow.

CVE-2015-8396 has been assigned by cve@mitre.org to track the vulnerability - currently rated as CRITICAL severity.

CVSS3 Score: 10 - CRITICAL

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
CHANGED	HIGH	HIGH	HIGH

CVSS2 Score: 10 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
Full Disclosure: CVE-2015-8396: GDCM buffer overflow in ImageRegionReader::ReadIntoBuffer	seclists.org text/html	FULLDISC 20160111 CVE-2015-8396: GDCM buffer overflow in ImageRegionReader::ReadIntoBuffer

Grassroots DICOM / Re: [Gdcm2] GDCM <2.6.1 two vulnerabilites	Exploit sourceforge.net text/html	MLIST [gdcm-developers] 20151221 Re: [Gdcm2] GDCM <2.6.1 two vulnerabilites
Grassroots DICOM / Gdcm / Commit [e547b1]	sourceforge.net text/html	CONFIRM sourceforge.net/p/gdcm/gdcm/ci/e547b1ded3fd21e0b0ad149f13045aa12d4
SecurityFocus	www.securityfocus.com text/html	BUGTRAQ 20160111 CVE-2015-8396: GDCM buffer overflow in ImageRegionReader::ReadIntoBuffer
Grassroots DICOM (GDCM) 2.6.0 and 2.6.1 - ImageRegionReader::ReadIntoBuffer Buffer Overflow - Linux dos Exploit	www.exploit-db.com Proof of Concept text/html	EXPLOIT-DB 39229
CENSUS | GDCM buffer overflow in ImageRegionReader :: ReadIntoBuffer	Exploit census-labs.com text/html	MISC census-labs.com/news/2016/01/11/gdcm-buffer-overflow-imageregionreaderreadintobuffer/
GDCM 2.6.0 / 2.6.1 Integer Overflow ≈ Packet Storm	packetstormsecurity.com text/html	MISC packetstormsecurity.com/files/135205/GDCM-2.6.0-2.6.1-Integer-Overflow.html
Grassroots DICOM / [Gdcm2] GDCM <2.6.1 two vulnerabilites	Exploit sourceforge.net text/html	MLIST [gdcm-developers] 20151204 [Gdcm2] GDCM <2.6.1 two vulnera

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Grassroots Dicom Project	Grassroots Dicom	2.6.1	All	All	All
Application	Grassroots Dicom Project	Grassroots Dicom	2.6.1	All	All	All
Application	Grassroots Dicom Project	Grassroots Dicom	All	All	All	All

cpe:2.3:a:grassroots_dicom_project:grassroots_dicom:2.6.1:*:*:*:*:*:*:*:

cpe:2.3:a:grassroots_dicom_project:grassroots_dicom:2.6.1:*:*:*:*:*:*:*:

cpe:2.3:a:grassroots_dicom_project:grassroots_dicom:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report