



CVE-2014-2072

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

Summary

CVE	CVE-2014-2072
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-01-08 16:15:00 UTC
Updated	2020-01-17 15:24:00 UTC
Description	Dassault Systemes Catia V5-6R2013: Stack Buffer Overflow due to inadequate boundary checks

Risk And Classification

Problem Types: CWE-787

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	3ds	Catia	v5-6r2013	All	All	All
Application	3ds	Catia	v5-6r2013	All	All	All

References

Reference	Source	Link	Tags
Catia V5-6R2013 Stack Buffer Overflow ≈ Packet Storm	MISC	packetstormsecurity.com	Exploit, Thi
Dassault Systemes Catia Stack Buffer Overflow Vulnerability - Exploit-Database.net	EXPLOIT-DB	www.exploit-database.net	Exploit, Thi
Dassault Systemes Catia Stack Buffer Overflow Vulnerability	MISC	www.securityfocus.com	Third Party
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical,

No vendor comments have been submitted for this CVE.

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

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](#).

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