CVE-2013-7299

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2013-7299
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-01-26 20:55:00 UTC
Updated	2017-08-29 01:34:00 UTC
Description	framework/common/messageheaderparser.cpp in Tntnet before 2.2.1 allows remote attackers to obtain sensitive informatio

Risk And Classification

Problem Types: CWE-200

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Tntnet	Tntnet	2.0	All	All	All
Application	Tntnet	Tntnet	2.1	All	All	All
Application	Tntnet	Tntnet	2.0	All	All	All
Application	Tntnet	Tntnet	2.1	All	All	All
Application	Tntnet	Tntnet	All	All	All	All

References

Reference	Source	Link	Tags
Security Advisory SA56400 - Tntnet HTTP Header Disclosure Vulnerability - Secunia	SECUNIA	secunia.com	Vendo
fix possible information leak · maekitalo/tntnet@9bd3b14 · GitHub	CONFIRM	github.com	Patch
www.tntnet.org/download/tntnet-2.2.1/Releasenotes-2.2.1.markdown	CONFIRM	www.tntnet.org	
Tntnet CVE-2013-7299 Information Disclosure Vulnerability	BID	www.securityfocus.com	
oss-sec: CVE requests / advisory: cxxtools <= 2.2, Tntnet <= 2.2	MLIST	seclists.org	
oss-sec: Re: CVE requests / advisory: cxxtools <= 2.2, Tntnet <= 2.2	MLIST	seclists.org	
IBM X-Force Exchange	XF	exchange.xforce.ibmcloud.com	
[SECURITY] Fedora 20 Update: tntnet-2.2.1-2.fc20	FEDORA	lists.fedoraproject.org	
CVE Program record	CVE.ORG	www.cve.org	canoni

NVD vulnerability detail	NVD	nvd.nist.gov	canoni

No vendor comments have been submitted for this CVE.

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

Free CVE JSON API cve.report/api

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