



CVE-2004-2534

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

Summary

CVE	CVE-2004-2534
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2004-12-31 05:00:00 UTC
Updated	2017-07-11 01:31:00 UTC
Description	Fastream NETFile Server 7.1.2 does not properly handle keep-alive connection timeouts and does not close the connection

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Fastream	Netfile Server	6.5.1.980	All	All	All
Application	Fastream	Netfile Server	6.5.1.981	All	All	All
Application	Fastream	Netfile Server	6.7.2.1085	All	All	All
Application	Fastream	Netfile Server	6.7.3	All	All	All
Application	Fastream	Netfile Server	6.7.5	All	All	All
Application	Fastream	Netfile Server	7.1	All	All	All
Application	Fastream	Netfile Server	7.1.2	All	All	All
Application	Fastream	Netfile Server	7.1.2	All	professional	All
Application	Fastream	Netfile Server	6.5.1.980	All	All	All
Application	Fastream	Netfile Server	6.5.1.981	All	All	All
Application	Fastream	Netfile Server	6.7.2.1085	All	All	All
Application	Fastream	Netfile Server	6.7.3	All	All	All
Application	Fastream	Netfile Server	6.7.5	All	All	All
Application	Fastream	Netfile Server	7.1	All	All	All
Application	Fastream	Netfile Server	7.1.2	All	All	All
Application	Fastream	Netfile Server	7.1.2	All	professional	All

References	
Reference	Source
Fastream NETFile Server HEAD Connection Errors Let Remote Users Consume All Available Connections - SecurityTracker	SECTrack
Secunia - Advisories - Fastream NETFile FTP/Web Server Multiple HEAD Requests Denial of Service	SECUNIA
IBM X-Force Exchange	XF
12101	OSVDB
Fastream NetFile FTP/Web Server HEAD Request Denial Of Service Vulnerability	BID
Security Advisory B003	MISC
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD
No vendor comments have been submitted for this CVE.	
There are currently no legacy QID mappings associated with this CVE.	