



CVE-2015-1965

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

Summary

CVE	CVE-2015-1965
State	PUBLISHED
Assigner	ibm
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-06-30 15:59:15 UTC
Updated	2026-05-06 22:30:45 UTC
Description	Stack-based buffer overflow in the server in IBM Tivoli Storage Manager FastBack 6.1 before 6.1.12 allows remote attacker

Risk And Classification

Primary CVSS: v2.0 7.8 from nvd@nist.gov

AV:N/AC:L/Au:N/C:N/I:N/A:C

Problem Types: CWE-119 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

None

Integrity

None

Availability

Complete

AV:N/AC:L/Au:N/C:N/I:N/A:C

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	ibm	Tivoli Storage Manager Fastback	6.1.0.0	All	All	All

Application	Ibm	Tivoli Storage Manager Fastback	6.1.1.0	All	All	All
Application	Ibm	Tivoli Storage Manager Fastback	6.1.10.0	All	All	All
Application	Ibm	Tivoli Storage Manager Fastback	6.1.10.1	All	All	All
Application	Ibm	Tivoli Storage Manager Fastback	6.1.11.0	All	All	All
Application	Ibm	Tivoli Storage Manager Fastback	6.1.11.1	All	All	All
Application	Ibm	Tivoli Storage Manager Fastback	6.1.7.2	All	All	All
Application	Ibm	Tivoli Storage Manager Fastback	6.1.8.0	All	All	All
Application	Ibm	Tivoli Storage Manager Fastback	6.1.8.1	All	All	All
Application	Ibm	Tivoli Storage Manager Fastback	6.1.9.0	All	All	All
Application	Ibm	Tivoli Storage Manager Fastback	6.1.9.1	All	All	All

Vendor Declared Affected Products				
Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

References	
Reference	Source
IBM Tivoli Storage Manager FastBack Multiple Flaws Let Remote Users Deny Service and Execute Arbitrary Code - SecurityTracker	af854e
Malformed Request	af854e
IBM Security Bulletin: Multiple Security Vulnerabilities in IBM Tivoli Storage Manager FastBack - United States	af854e
CVE Program record	CVE.C
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

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