



CVE-2010-3755

Published on: 10/05/2010 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:02 PM UTC

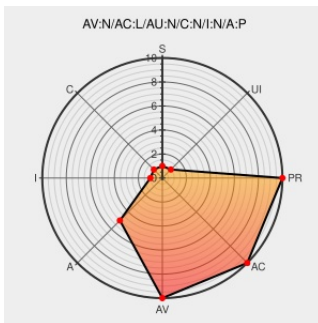
CVE-2010-3755

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of **Tivoli Storage Manager Fastback** from **Ibm** contain the following vulnerability:

The `_DAS_ReadBlockReply` function in `FastBackServer.exe` in the Server in IBM Tivoli Storage Manager (TSM) FastBack 5.5.0.0 through 5.5.6.0 and 6.1.0.0 through 6.1.0.1 allows remote attackers to cause a denial of service (NULL pointer dereference and daemon crash) via data in a TCP packet. NOTE: this might overlap CVE-2010-3060.

CVE-2010-3755 has been assigned by [M cve@mitre.org](mailto:cve@mitre.org) to track the vulnerability

CVSS2 Score: **5 - MEDIUM**

Access
Vector

NETWORK

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

NONE

Integrity
Impact

NONE

Availability
Impact

PARTIAL

CVE References

Description

Tags

Link

SecurityFocus

[www.securityfocus.com
text/html](http://www.securityfocus.com/text/html)

[BUGTRAQ 20100929 ZDI-10-187: IBM TSM FastBack Server _DAS_ReadBlockReply Remote Denial of Service Vulnerability](#)

IBM notice: The page you requested cannot be displayed

[Vendor Advisory](#)
[www-01.ibm.com
text/html](http://www-01.ibm.com/text/html)
Inactive Link **Not Archived**

[AIXAPAR IC69883](#)

Zero Day Initiative

[zerodayinitiative.com
text/html](http://zerodayinitiative.com/text/html)

[MISC zerodayinitiative.com/advisories/ZDI-10-187/](http://MISC.zerodayinitiative.com/advisories/ZDI-10-187/)

Security fixes available for IBM Tivoli Storage Manager FastBack

[Vendor Advisory](#)
[www.ibm.com
text/html](http://www.ibm.com/text/html)

[CONFIRM www.ibm.com/support/docview.wss?uid=swg21443820](#)

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Ibm	Tivoli Storage Manager Fastback	5.5.0	All	All	All
Application	Ibm	Tivoli Storage Manager Fastback	5.5.1	All	All	All
Application	Ibm	Tivoli Storage Manager Fastback	5.5.2	All	All	All
Application	Ibm	Tivoli Storage Manager Fastback	5.5.2.0	All	All	All
Application	Ibm	Tivoli Storage Manager Fastback	5.5.3.0	All	All	All
Application	Ibm	Tivoli Storage Manager Fastback	5.5.4.0	All	All	All
Application	Ibm	Tivoli Storage Manager Fastback	5.5.5.0	All	All	All
Application	Ibm	Tivoli Storage Manager Fastback	5.5.6.0	All	All	All
Application	Ibm	Tivoli Storage Manager Fastback	6.1.0.0	All	All	All
Application	Ibm	Tivoli Storage Manager Fastback	6.1.0.1	All	All	All
Application	Ibm	Tivoli Storage Manager Fastback	5.5.0	All	All	All
Application	Ibm	Tivoli Storage Manager Fastback	5.5.1	All	All	All
Application	Ibm	Tivoli Storage Manager Fastback	5.5.2	All	All	All
Application	Ibm	Tivoli Storage Manager Fastback	5.5.2.0	All	All	All
Application	Ibm	Tivoli Storage Manager Fastback	5.5.3.0	All	All	All
Application	Ibm	Tivoli Storage Manager Fastback	5.5.4.0	All	All	All
Application	Ibm	Tivoli Storage Manager Fastback	5.5.5.0	All	All	All
Application	Ibm	Tivoli Storage Manager Fastback	5.5.6.0	All	All	All
Application	Ibm	Tivoli Storage Manager Fastback	6.1.0.0	All	All	All
Application	Ibm	Tivoli Storage Manager Fastback	6.1.0.1	All	All	All

```
cpe:2.3:a:ibm:tivoli storage manager fastback:5.5.0:*.~*~*~*~*~*~*
```

```
cpe:2.3:a:ibm:tivoli storage manager fastback:5.5.1:*.***.***.*
```

```
cpe:2.3:a:ibm:tivoli storage manager fastback:5.5.2:*:*:*:*:*.*
```

```
cpe:2.3:a:ibm:tivoli storage manager fastback:5.5.2.0:*:*:*:*:*.*
```

```
cpe:2.3:a:ibm:tivoli storage manager fastback:5.5.3.0:*:*:*:*:*.*
```

```
cpe:2.3:a:ibm:tivoli storage manager fastback:5.5.4.0:*:*:*:*:*:
```

cpe:2.3:a:ibm:tivoli_storage_manager_fastback:5.5.5.0:*****:
cpe:2.3:a:ibm:tivoli_storage_manager_fastback:5.5.6.0:*****:
cpe:2.3:a:ibm:tivoli_storage_manager_fastback:6.1.0.0:*****:
cpe:2.3:a:ibm:tivoli_storage_manager_fastback:6.1.0.1:*****:
cpe:2.3:a:ibm:tivoli_storage_manager_fastback:5.5.0:*****:
cpe:2.3:a:ibm:tivoli_storage_manager_fastback:5.5.1:*****:
cpe:2.3:a:ibm:tivoli_storage_manager_fastback:5.5.2:*****:
cpe:2.3:a:ibm:tivoli_storage_manager_fastback:5.5.2.0:*****:
cpe:2.3:a:ibm:tivoli_storage_manager_fastback:5.5.3.0:*****:
cpe:2.3:a:ibm:tivoli_storage_manager_fastback:5.5.4.0:*****:
cpe:2.3:a:ibm:tivoli_storage_manager_fastback:5.5.5.0:*****:
cpe:2.3:a:ibm:tivoli_storage_manager_fastback:5.5.6.0:*****:
cpe:2.3:a:ibm:tivoli_storage_manager_fastback:6.1.0.0:*****:
cpe:2.3:a:ibm:tivoli_storage_manager_fastback:6.1.0.1:*****:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

© [CVE.report](#) 2023   |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, 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](#)