



# CVE-2004-1663

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

## Summary

<b>CVE</b>	CVE-2004-1663
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2004-09-04 04:00:00 UTC
<b>Updated</b>	2021-06-22 15:19:00 UTC
<b>Description</b>	Engenio/LSI Logic storage controllers, as used in products such as Storagetek D280, and IBM DS4100 (formerly FastT 100

## Risk And Classification

**Problem Types:** NVD-CWE-Other

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Broadcom</a>	<a href="#">Fabric Operating System</a>	2.1.2	All	All	All
Operating System	<a href="#">Broadcom</a>	<a href="#">Fabric Operating System</a>	2.2	All	All	All
Operating System	<a href="#">Broadcom</a>	<a href="#">Fabric Operating System</a>	3.1	All	All	All
Operating System	<a href="#">Brocade</a>	<a href="#">Fabric Os</a>	2.1.2	All	All	All
Operating System	<a href="#">Brocade</a>	<a href="#">Fabric Os</a>	2.2	All	All	All
Operating System	<a href="#">Brocade</a>	<a href="#">Fabric Os</a>	3.1	All	All	All
Operating System	<a href="#">Brocade</a>	<a href="#">Fabric Os</a>	2.1.2	All	All	All
Operating System	<a href="#">Brocade</a>	<a href="#">Fabric Os</a>	2.2	All	All	All
Operating System	<a href="#">Brocade</a>	<a href="#">Fabric Os</a>	3.1	All	All	All
Hardware	<a href="#">Brocade</a>	<a href="#">Silkworm</a>	3200	All	All	All
Hardware	<a href="#">Brocade</a>	<a href="#">Silkworm</a>	3250	All	All	All
Hardware	<a href="#">Brocade</a>	<a href="#">Silkworm</a>	3800	All	All	All
Hardware	<a href="#">Brocade</a>	<a href="#">Silkworm</a>	3850	All	All	All
Hardware	<a href="#">Brocade</a>	<a href="#">Silkworm</a>	3900	All	All	All
Hardware	<a href="#">Brocade</a>	<a href="#">Silkworm</a>	3200	All	All	All
Hardware	<a href="#">Brocade</a>	<a href="#">Silkworm</a>	3250	All	All	All
Hardware	<a href="#">Brocade</a>	<a href="#">Silkworm</a>	3800	All	All	All

Hardware	<a href="#">Brocade</a>	<a href="#">Silkworm</a>	3850	All	All	All
Hardware	<a href="#">Brocade</a>	<a href="#">Silkworm</a>	3900	All	All	All
Hardware	<a href="#">Brocade</a>	<a href="#">Silkworm Fiber Channel Switch</a>	2010	All	All	All
Hardware	<a href="#">Brocade</a>	<a href="#">Silkworm Fiber Channel Switch</a>	2040	All	All	All
Hardware	<a href="#">Brocade</a>	<a href="#">Silkworm Fiber Channel Switch</a>	2050	All	All	All
Hardware	<a href="#">Brocade</a>	<a href="#">Silkworm Fiber Channel Switch</a>	2010	All	All	All
Hardware	<a href="#">Brocade</a>	<a href="#">Silkworm Fiber Channel Switch</a>	2040	All	All	All
Hardware	<a href="#">Brocade</a>	<a href="#">Silkworm Fiber Channel Switch</a>	2050	All	All	All
Hardware	<a href="#">Engenio</a>	<a href="#">Storage Controller</a>	2822	All	All	All
Hardware	<a href="#">Engenio</a>	<a href="#">Storage Controller</a>	2882	All	All	All
Hardware	<a href="#">Engenio</a>	<a href="#">Storage Controller</a>	4884	All	All	All
Hardware	<a href="#">Engenio</a>	<a href="#">Storage Controller</a>	5884	All	All	All
Hardware	<a href="#">Engenio</a>	<a href="#">Storage Controller</a>	2822	All	All	All
Hardware	<a href="#">Engenio</a>	<a href="#">Storage Controller</a>	2882	All	All	All
Hardware	<a href="#">Engenio</a>	<a href="#">Storage Controller</a>	4884	All	All	All
Hardware	<a href="#">Engenio</a>	<a href="#">Storage Controller</a>	5884	All	All	All
Hardware	<a href="#">Ibm</a>	<a href="#">Ds4100</a>	All	All	All	All
Hardware	<a href="#">Ibm</a>	<a href="#">Ds4100</a>	All	All	All	All
Hardware	<a href="#">Storagetek</a>	<a href="#">D280</a>	All	All	All	All
Hardware	<a href="#">Storagetek</a>	<a href="#">D280</a>	All	All	All	All

## References

Reference	Source	Link	Tags
'Engenio/LSI Logic controllers denial of service/data corruption' - MARC	BUGTRAQ	<a href="#">marc.info</a>	
Secunia - Advisories - Engenio Storage Controllers Denial of Service Vulnerability	SECUNIA	<a href="#">secunia.com</a>	Vendor A
IBM X-Force Exchange	XF	<a href="#">exchange.xforce.ibmcloud.com</a>	
Engenio Storage Controller Remote Denial Of Service Vulnerability	BID	<a href="#">www.securityfocus.com</a>	Vendor A
CVE Program record	CVE.ORG	<a href="#">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="#">nvd.nist.gov</a>	canonical

No vendor comments have been submitted for this CVE.

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

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](#)**