



# CVE-2014-9143

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

## Summary

<b>CVE</b>	CVE-2014-9143
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2014-12-05 15:59:00 UTC
<b>Updated</b>	2018-10-09 19:54:00 UTC
<b>Description</b>	Open redirect vulnerability in Technicolor Router TD5130 with firmware 2.05.C29GV allows remote attackers to redirect use

## Risk And Classification

**Problem Types:** CWE-17

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Technicolor	Td5130 Router Firmware	2.05.c29gv	All	All	All
Operating System	Technicolor	Td5130 Router Firmware	2.05.c29gv	All	All	All

## References

Reference	Source	Link	Tags
Technicolor DT5130 2.05.C29GV - Multiple Vulnerabilities	EXPLOIT-DB	<a href="http://www.exploit-db.com">www.exploit-db.com</a>	Exploit
ADSL2+ 2.05.C29GV XSS / URL Redirect / Command Injection ≈ Packet Storm	MISC	<a href="http://packetstormsecurity.com">packetstormsecurity.com</a>	Exploit
SecurityFocus	BUGTRAQ	<a href="http://www.securityfocus.com">www.securityfocus.com</a>	
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>	canonical, analy

No vendor comments have been submitted for this CVE.

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

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](#)**