



CVE-2014-5437

Published on: 12/17/2014 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:52 PM UTC

CVE-2014-5437

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



Certain versions of [Touchstone Tg862g/ct](#) from [Arris](#) contain the following vulnerability:

Multiple cross-site request forgery (CSRF) vulnerabilities in ARRIS Touchstone TG862G/CT Telephony Gateway with firmware 7.6.59S.CT and earlier allow remote attackers to hijack the authentication of administrators for requests that (1) enable remote management via a request to `remote_management.php`, (2) add a port forwarding rule via a request to `port_forwarding_add.php`, (3) change the wireless network to open via a request to `wireless_network_configuration_edit.php`, or (4) conduct cross-site scripting (XSS) attacks via the keyword parameter to `managed_sites_add_keyword.php`.

CVE-2014-5437 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **6.8 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Full Disclosure: CVE-2014-5437: Arris TG862G - Cross-site Request Forgery (CSRF)	seclists.org text/html	FULLDISC 20141216 CVE-2014-5437: Arris TG862G - Cross-site Request Forgery (CSRF)
Full Disclosure: CVE-2014-5438: Arris TG862G - Cross-site Scripting (XSS)	web.archive.org text/html Inactive Link Not Archived	FULLDISC 20141216 CVE-2014-5438: Arris TG862G - Cross-site Scripting (XSS)

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 warrant the accuracy of the information provided on these sites. CVEreport is not responsible for any damage or loss resulting from the use of the information provided on these sites.

CVE-report 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
Hardware 	Arris	Touchstone Tg862g/ct	All	All	All	All
Application	Arris	Touchstone Tg862g/ct Firmware	All	All	All	All
Hardware 	Arris	Touchstone Tg862g/ct	All	All	All	All
Hardware 	Arris	Touchstone Tg862g/ct	All	All	All	All
Application	Arris	Touchstone Tg862g/ct Firmware	All	All	All	All
cpe:2.3:h:arris:touchstone_tg862g/ct:*****:						
cpe:2.3:a:arris:touchstone_tg862g/ct_firmware:*****:						
cpe:2.3:h:arris:touchstone_tg862g\ct:*****:						
cpe:2.3:h:arris:touchstone_tg862g\ct:*****:						
cpe:2.3:a:arris:touchstone_tg862g\ct_firmware:*****:						

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