



CVE-2020-15043

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

Summary

CVE	CVE-2020-15043
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-06-29 18:15:00 UTC
Updated	2020-07-06 18:35:00 UTC
Description	iBall WRB303N devices allow CSRF attacks, as demonstrated by enabling remote management, enabling DHCP, or modify

Risk And Classification

Problem Types: CWE-352

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Iball	Wrb303n	-	All	All	All
Hardware	Iball	Wrb303n	-	All	All	All
Operating System	Iball	Wrb303n Firmware	-	All	All	All
Operating System	Iball	Wrb303n Firmware	-	All	All	All

References

Reference

- [GitHub - Saket-taneja/IballCSRFExploit: Cross Site request forgery attack On IBall router WRB303N allows to modify IP subnets and other me](#)
- [Iball CSRF Exploit · GitHub](#)
- [CVE Program record](#)
- [NVD vulnerability detail](#)

No vendor comments have been submitted for this CVE.

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

© [CVE.report](#) 2026 |

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](#)