



CVE-2022-25915

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

Summary

CVE	CVE-2022-25915
State	PUBLIC
Assigner	vultures@jpcert.or.jp
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-03-31 09:15:00 UTC
Updated	2023-08-08 14:21:00 UTC
Description	Improper access control vulnerability in ELECOM LAN routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Elecom	Edwrc-2533gst2	-	All	All	All
Operating System	Elecom	Edwrc-2533gst2 Firmware	All	All	All	All
Hardware	Elecom	Wmc-2hc-w	-	All	All	All
Operating System	Elecom	Wmc-2hc-w Firmware	All	All	All	All
Hardware	Elecom	Wmc-c2533gst-w	-	All	All	All
Operating System	Elecom	Wmc-c2533gst-w Firmware	All	All	All	All
Hardware	Elecom	Wmc-dlgst2-w	-	All	All	All
Operating System	Elecom	Wmc-dlgst2-w Firmware	All	All	All	All
Hardware	Elecom	Wmc-m1267gst2-w	-	All	All	All
Operating System	Elecom	Wmc-m1267gst2-w Firmware	All	All	All	All
Hardware	Elecom	Wrc-1167gs2-b	-	All	All	All
Operating System	Elecom	Wrc-1167gs2-b Firmware	All	All	All	All
Hardware	Elecom	Wrc-1167gs2h-b	-	All	All	All
Operating System	Elecom	Wrc-1167gs2h-b Firmware	All	All	All	All
Hardware	Elecom	Wrc-1167gst2	-	All	All	All
Hardware	Elecom	Wrc-1167gst2a	-	All	All	All
Operating System	Elecom	Wrc-1167gst2a Firmware	All	All	All	All

Hardware	Elecom	Wrc-1167gst2h	-	All	All	All
Operating System	Elecom	Wrc-1167gst2h Firmware	All	All	All	All
Operating System	Elecom	Wrc-1167gst2 Firmware	All	All	All	All
Hardware	Elecom	Wrc-1750gs	-	All	All	All
Hardware	Elecom	Wrc-1750gst2	-	All	All	All
Operating System	Elecom	Wrc-1750gst2 Firmware	All	All	All	All
Hardware	Elecom	Wrc-1750gsv	-	All	All	All
Operating System	Elecom	Wrc-1750gsv Firmware	All	All	All	All
Operating System	Elecom	Wrc-1750gs Firmware	All	All	All	All
Hardware	Elecom	Wrc-1900gst	-	All	All	All
Hardware	Elecom	Wrc-1900gst2	-	All	All	All
Hardware	Elecom	Wrc-1900gst2sp	-	All	All	All
Operating System	Elecom	Wrc-1900gst2sp Firmware	All	All	All	All
Operating System	Elecom	Wrc-1900gst2 Firmware	All	All	All	All
Operating System	Elecom	Wrc-1900gst Firmware	All	All	All	All
Hardware	Elecom	Wrc-2533gs2-b	-	All	All	All
Operating System	Elecom	Wrc-2533gs2-b Firmware	All	All	All	All
Hardware	Elecom	Wrc-2533gs2-w	-	All	All	All
Operating System	Elecom	Wrc-2533gs2-w Firmware	All	All	All	All
Hardware	Elecom	Wrc-2533gst	-	All	All	All
Hardware	Elecom	Wrc-2533gst2	-	All	All	All
Hardware	Elecom	Wrc-2533gst2-g	-	All	All	All
Operating System	Elecom	Wrc-2533gst2-g Firmware	All	All	All	All
Hardware	Elecom	Wrc-2533gst2sp	-	All	All	All
Operating System	Elecom	Wrc-2533gst2sp Firmware	All	All	All	All
Operating System	Elecom	Wrc-2533gst2 Firmware	All	All	All	All
Hardware	Elecom	Wrc-2533gsta	-	All	All	All
Operating System	Elecom	Wrc-2533gsta Firmware	All	All	All	All
Operating System	Elecom	Wrc-2533gst Firmware	All	All	All	All

References						
Reference						Source
無線LANルーターのセキュリティ向上のためのファームウェアアップデートのお願い - 最新情報 - セキュリティ情報 ELECOM						MISC
JVN#88993473: Multiple vulnerabilities in multiple ELECOM LAN routers						MISC
CVE Program record						CVE.ORG
NVD - National Vulnerability Database						NVD

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](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)