



CVE-2021-22283

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2021-22283
State	PUBLIC
Assigner	cybersecurity@ch.abb.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-02-28 05:15:00 UTC
Updated	2023-11-07 03:30:00 UTC
Description	Improper Initialization vulnerability in ABB Relion protection relays - 611 series, ABB Relion protection relays - 615 series IE

Risk And Classification

Problem Types: CWE-665

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Abb	Evd4	-	All	All	All
Operating System	Abb	Evd4 Firmware	All	All	All	All
Hardware	Abb	Rec615	-	All	All	All
Operating System	Abb	Rec615 Firmware	All	All	All	All
Hardware	Abb	Red615 lec	1.1	All	All	All
Operating System	Abb	Red615 lec Firmware	All	All	All	All
Hardware	Abb	Ref615r	-	All	All	All
Operating System	Abb	Ref615r Firmware	All	All	All	All
Hardware	Abb	Ref615 Ansi	1.0	All	All	All
Hardware	Abb	Ref615 Ansi	1.1	All	All	All
Operating System	Abb	Ref615 Ansi Firmware	All	All	All	All
Hardware	Abb	Ref615 lec	1.0	All	All	All
Hardware	Abb	Ref615 lec	1.1	All	All	All
Operating System	Abb	Ref615 lec Firmware	All	All	All	All
Hardware	Abb	Relion 611	-	All	All	All
Operating System	Abb	Relion 611 Firmware	All	All	All	All
Hardware	Abb	Relion 615 Ansi	2.0	All	All	All

Hardware	Abb	Relion 615 Ansi	4.0	-	All	All
Hardware	Abb	Relion 615 Ansi	4.0	fp1	All	All
Hardware	Abb	Relion 615 Ansi	4.0	fp2	All	All
Hardware	Abb	Relion 615 Ansi	5.0	fp1	All	All
Operating System	Abb	Relion 615 Ansi Firmware	All	All	All	All
Hardware	Abb	Relion 615 Cn	2.0	All	All	All
Hardware	Abb	Relion 615 Cn	3.0	All	All	All
Hardware	Abb	Relion 615 Cn	3.1	All	All	All
Hardware	Abb	Relion 615 Cn	4.0	-	All	All
Hardware	Abb	Relion 615 Cn	4.0	fp1	All	All
Hardware	Abb	Relion 615 Cn	5.0	fp1	All	All
Operating System	Abb	Relion 615 Cn Firmware	All	All	All	All
Hardware	Abb	Relion 615 lec	2.0	All	All	All
Hardware	Abb	Relion 615 lec	3.0	All	All	All
Hardware	Abb	Relion 615 lec	4.0	-	All	All
Hardware	Abb	Relion 615 lec	4.0	fp1	All	All
Hardware	Abb	Relion 615 lec	5.0	-	All	All
Hardware	Abb	Relion 615 lec	5.0	fp1	All	All
Operating System	Abb	Relion 615 lec Firmware	All	All	All	All
Hardware	Abb	Relion 620 Ansi	-	All	All	All
Operating System	Abb	Relion 620 Ansi Firmware	All	All	All	All
Hardware	Abb	Relion 620 Cn	2.0	-	All	All
Hardware	Abb	Relion 620 Cn	2.0	fp1	All	All
Operating System	Abb	Relion 620 Cn Firmware	All	All	All	All
Hardware	Abb	Relion 620 lec	2.0	-	All	All
Hardware	Abb	Relion 620 lec	2.0	fp1	All	All
Operating System	Abb	Relion 620 lec Firmware	All	All	All	All
Hardware	Abb	Rer615	-	All	All	All
Operating System	Abb	Rer615 Firmware	All	All	All	All
Hardware	Abb	Rer620	-	All	All	All
Operating System	Abb	Rer620 Firmware	All	All	All	All
Hardware	Abb	Rex640 Pcl1	-	All	All	All
Operating System	Abb	Rex640 Pcl1 Firmware	All	All	All	All
Hardware	Abb	Rex640 Pcl2	-	All	All	All
Operating System	Abb	Rex640 Pcl2 Firmware	All	All	All	All

Hardware	Abb	Rex640 Pcl3	-	All	All	All
Operating System	Abb	Rex640 Pcl3 Firmware	All	All	All	All
Hardware	Abb	Smu615	-	All	All	All
Operating System	Abb	Smu615 Firmware	All	All	All	All

References

Reference	Source	Link	Tags
search.abb.com/library/Download.aspx	MISC	search.abb.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

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