



CVE-2023-4299

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

Summary

CVE	CVE-2023-4299
State	PUBLIC
Assigner	ics-cert@hq.dhs.gov
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-08-31 21:15:00 UTC
Updated	2023-09-06 20:13:00 UTC
Description	Digi RealPort Protocol is vulnerable to a replay attack that may allow an attacker to bypass authentication to access connect

Risk And Classification

Problem Types: CWE-836

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Digi	Cm	-	All	All	All
Operating System	Digi	Cm Firmware	-	All	All	All
Hardware	Digi	Connectport Lts 8/16/32	-	All	All	All
Operating System	Digi	Connectport Lts 8/16/32 Firmware	All	All	All	All
Hardware	Digi	Connectport Ts 8/16	-	All	All	All
Operating System	Digi	Connectport Ts 8/16 Firmware	All	All	All	All
Hardware	Digi	Connect Es	-	All	All	All
Operating System	Digi	Connect Es Firmware	All	All	All	All
Hardware	Digi	Connect Sp	-	All	All	All
Operating System	Digi	Connect Sp Firmware	-	All	All	All
Hardware	Digi	One la	-	All	All	All
Hardware	Digi	One lap	-	All	All	All
Operating System	Digi	One lap Firmware	-	All	All	All
Operating System	Digi	One la Firmware	-	All	All	All
Hardware	Digi	One Sp	-	All	All	All
Operating System	Digi	One Sp Firmware	-	All	All	All
Hardware	Digi	One Sp la	-	All	All	All

Operating System	Digi	One Sp Ia Firmware	-	All	All	All
Hardware	Digi	Passport	-	All	All	All
Operating System	Digi	Passport Firmware	-	All	All	All
Hardware	Digi	Portserver Ts	-	All	All	All
Operating System	Digi	Portserver Ts Firmware	-	All	All	All
Hardware	Digi	Portserver Ts Mei	-	All	All	All
Operating System	Digi	Portserver Ts Mei Firmware	-	All	All	All
Hardware	Digi	Portserver Ts Mei Hardened	-	All	All	All
Operating System	Digi	Portserver Ts Mei Hardened Firmware	-	All	All	All
Hardware	Digi	Portserver Ts M Mei	-	All	All	All
Operating System	Digi	Portserver Ts M Mei Firmware	-	All	All	All
Hardware	Digi	Portserver Ts P Mei	-	All	All	All
Operating System	Digi	Portserver Ts P Mei Firmware	-	All	All	All
Application	Digi	Realport	All	All	All	All
Application	Digi	Realport	All	All	All	All
Hardware	Digi	Transport Wr11 Xt	-	All	All	All
Operating System	Digi	Transport Wr11 Xt Firmware	-	All	All	All
Hardware	Digi	Wr21	-	All	All	All
Operating System	Digi	Wr21 Firmware	-	All	All	All
Hardware	Digi	Wr31	-	All	All	All
Operating System	Digi	Wr31 Firmware	-	All	All	All
Hardware	Digi	Wr44 R	-	All	All	All
Operating System	Digi	Wr44 R Firmware	-	All	All	All

References

Reference	Source	Link	Tags
Digi RealPort Protocol CISA	MISC	www.cisa.gov	
www.digi.com/getattachment/resources/security/alerts/realport-cves/Dragos-...	MISC	www.digi.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](#).

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

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