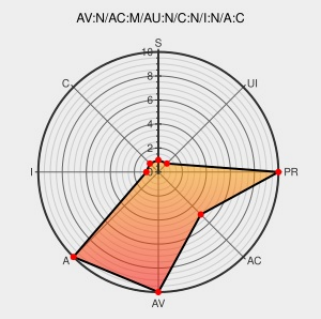
CVE-2013-2821

Published on: 12/21/2013 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:42 PM UTC

CVE-2013-2821

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Orion5r Dnp Master from Novatech contain the following vulnerability:

NovaTech Orion Substation Automation Platform OrionLX DNP Master 1.27.38 and DNP Slave 1.23.10 and earlier and Orion5/Orion5r DNP Master 1.27.38 and DNP Slave 1.23.10 and earlier allow remote attackers to cause a denial of service (driver crash and process restart) via a crafted DNP3 TCP packet.

CVE-2013-2821 has been assigned by ics-cert@hq.dhs.gov to track the vulnerability

CVSS2 Score: 7.1 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	NONE	COMPLETE

CVE References

Description	Tags	Link
NovaTech Orion DNP3 Improper Input Validation Vulnerability | ICS-CERT	US Government Resource ics-cert.us-cert.gov text/html	MISC ics-cert.us-cert.gov/advisories/ICSA-13-352-01

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Novatech	Orion5r Dnp Master	1.27.38	All	All	All
Hardware	Novatech	Orion5r Dnp Master	1.27.38	All	All	All
Hardware	Novatech	Orion5r Dnp Slave	1.23.10	All	All	All
Hardware	Novatech	Orion5r Dnp Slave	1.23.10	All	All	All
Hardware	Novatech	Orion5 Dnp Master	1.27.38	All	All	All
Hardware	Novatech	Orion5 Dnp Master	1.27.38	All	All	All
Hardware	Novatech	Orion5 Dnp Slave	1.23.10	All	All	All
Hardware	Novatech	Orion5 Dnp Slave	1.23.10	All	All	All
Hardware	Novatech	Orionlx Dnp Master	1.27.38	All	All	All
Hardware	Novatech	Orionlx Dnp Master	1.27.38	All	All	All
Hardware	Novatech	Orionlx Dnp Slave	1.23.10	All	All	All
Hardware	Novatech	Orionlx Dnp Slave	1.23.10	All	All	All

cpe:2.3:h:novatech:orion5r_dnp_master:1.27.38:*:*:*:*:*:*:*:

cpe:2.3:h:novatech:orion5r_dnp_master:1.27.38:*:*:*:*:*:*:*:

cpe:2.3:h:novatech:orion5r_dnp_slave:1.23.10:*:*:*:*:*:*:*:

cpe:2.3:h:novatech:orion5r_dnp_slave:1.23.10:*:*:*:*:*:*:*:

cpe:2.3:h:novatech:orion5_dnp_master:1.27.38:*:*:*:*:*:*:*:

cpe:2.3:h:novatech:orion5_dnp_master:1.27.38:*:*:*:*:*:*:*:

cpe:2.3:h:novatech:orion5_dnp_slave:1.23.10:*:*:*:*:*:*:*:

cpe:2.3:h:novatech:orion5_dnp_slave:1.23.10:*:*:*:*:*:*:*:

cpe:2.3:h:novatech:orionlx_dnp_master:1.27.38:*:*:*:*:*:*:*:

cpe:2.3:h:novatech:orionlx_dnp_master:1.27.38:*:*:*:*:*:*:*:

cpe:2.3:h:novatech:orionlx_dnp_slave:1.23.10:*:*:*:*:*:*:*:

cpe:2.3:h:novatech:orionlx_dnp_slave:1.23.10:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report