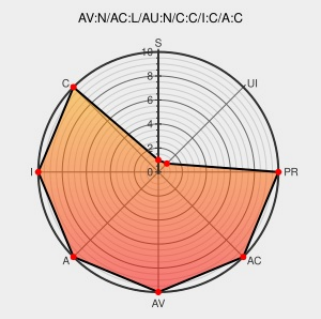
CVE-2013-2802

Published on: 08/21/2013 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:43 PM UTC

CVE-2013-2802

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



Certain versions of Rtu Firmware from Sixnet contain the following vulnerability:

The universal protocol implementation in Sixnet UDR before 2.0 and RTU firmware before 4.8 allows remote attackers to execute arbitrary code; read, modify, or create files; or obtain file metadata via function opcodes.

CVE-2013-2802 has been assigned by ics-cert@hq.dhs.gov to track the vulnerability

CVSS2 Score: 10 - HIGH

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

CVE References

Description	Tags	Link
Sixnet Universal Protocol Undocumented Function Codes | ICS-CERT	US Government Resource, ics-cert.us-cert.gov, text/html	MISC ics-cert.us-cert.gov/advisories/ICSA-13-231-01

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Sixnet	Rtu Firmware	All	All	All	All
Application	Sixnet	Udr	All	All	All	All

cpe:2.3:o:sixnet:rtu_firmware:*:*:*:*:*:*:*:*:

cpe:2.3:a:sixnet:udr:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→