CVE-2015-7288

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2015-7288
State	PUBLISHED
Assigner	certcc
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-11-25 04:59:06 UTC
Updated	2026-05-06 22:30:45 UTC
Description	CSL DualCom GPRS CS2300-R devices with firmware 1.25 through 3.53 allow remote attackers to modify the configuratior

Risk And Classification

Primary CVSS: v2.0 4.3 from nvd@nist.gov

AV:N/AC:M/Au:N/C:N/I:P/A:N

Problem Types: CWE-254 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

None

Confidentiality

None

Integrity

Partial

Availability

None

AV:N/AC:M/Au:N/C:N/I:P/A:N

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Csl Dualcom	Gprs	cs2300-r	All	All	All

Operating System	Csl Dualcom	Gprs Cs2300-r Firmware	1.25	All	All	All
Operating System	Csl Dualcom	Gprs Cs2300-r Firmware	3.53	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

References

Reference	Source
Vulnerability Note VU#428280 - CSL DualCom GPRS CS2300-R alarm signalling boards contain multiple vulnerabilties	af854a3a-2127-422
VU#428280 - CSL DualCom GPRS CS2300-R alarm signalling boards contain multiple vulnerabilties	af854a3a-2127-422
» CSL Dualcom CS2300-R signalling unit vulnerabilities	af854a3a-2127-422
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.