



CVE-2012-0314

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

Summary

CVE	CVE-2012-0314
State	PUBLISHED
Assigner	jpccert
Source Priority	CVE Program / NVD first with legacy fallback
Published	2012-02-03 04:05:51 UTC
Updated	2026-04-29 01:13:23 UTC
Description	Multiple cross-site request forgery (CSRF) vulnerabilities on the eAccess Pocket WiFi (aka GP02) router before 2.00 with fi

Risk And Classification

Primary CVSS: v2.0 6.8 from nvd@nist.gov

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

Problem Types: CWE-352 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

Partial

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Emobile	Pocket Wifi	All	All	All	All

Application	Emobile	Pocket Wifi Firmware	All	All	All	All
Vendor Declared Affected Products						
Source	Vendor	Product	Version	Platforms		
CNA	Na	N/a	affected n/a	Not specified		
References						
Reference						
Security Advisory SA47795 - Emobile Pocket WiFi GP02 Cross-Site Request Forgery Vulnerability - Secunia						
Pocket WiFi (GP02)をご利用のお客さまへ～ マルチSSID※への対応に伴う本体ファームウェアのバージョンアップについて ～ ～ イー ・ ・						
jvndb.jvn.jp/jvndb/JVNDB-2012-000010						
JVN#33021167: Pocket WiFi (GP02) vulnerable to cross-site request forgery						
Emobile Pocket WiFi GP02 Cross-Site Request Forgery Vulnerability						
CVE Program record						
NVD vulnerability detail						
No vendor comments have been submitted for this CVE.						
There are currently no legacy QID mappings associated with this CVE.						