CVE-2015-0877

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

Summary

CVE	CVE-2015-0877
State	PUBLIC
Assigner	vultures@jpcert.or.jp
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-04-06 01:59:00 UTC
Updated	2015-04-06 16:55:00 UTC
Description	Unrestricted file upload vulnerability in app/lib/mlf.pl in C-BOARD Moyuku before 1.03b3 allows remote attackers to execute

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	C-board Moyuku Project	C-board Moyuku	1.01	b1	All	All
Application	C-board Moyuku Project	C-board Moyuku	1.01	b2	All	All
Application	C-board Moyuku Project	C-board Moyuku	1.01	b3	All	All
Application	C-board Moyuku Project	C-board Moyuku	1.01	b4	All	All
Application	C-board Moyuku Project	C-board Moyuku	1.01	b6	All	All
Application	C-board Moyuku Project	C-board Moyuku	1.02	b1	All	All
Application	C-board Moyuku Project	C-board Moyuku	1.03	b1	All	All
Application	C-board Moyuku Project	C-board Moyuku	1.01	b1	All	All
Application	C-board Moyuku Project	C-board Moyuku	1.01	b2	All	All
Application	C-board Moyuku Project	C-board Moyuku	1.01	b3	All	All
Application	C-board Moyuku Project	C-board Moyuku	1.01	b4	All	All
Application	C-board Moyuku Project	C-board Moyuku	1.01	b6	All	All
Application	C-board Moyuku Project	C-board Moyuku	1.02	b1	All	All
Application	C-board Moyuku Project	C-board Moyuku	1.03	b1	All	All
Application	C-board Moyuku Project	C-board Moyuku	All	b2	All	All

References

Reference	Source	Link	Tags
JVN#73261710: C-BOARD Moyuku vulnerable to arbitrary file creation	JVN	jvn.jp	Vendor Advisory
JVNDB-2015-000018	JVNDB	jvndb.jvn.jp	Vendor Advisory
オープンソースプロジェクトニュース一覧 - C-BOARD Moyuku - SourceForge.JP	CONFIRM	sourceforge.jp	Vendor Advisory
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.