CVE-2005-1091

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

Summary

CVE	CVE-2005-1091
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2005-05-02 04:00:00 UTC
Updated	2025-04-03 01:03:51 UTC
Description	Maxthon 1.2.0 and 1.2.1 allows remote attackers to bypass the security ID and use restricted plugin API functions via script

Risk And Classification

Primary CVSS: v2.0 7.5 from nvd@nist.gov

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

Problem Types: NVD-CWE-Other | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

Partial

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Maxthon	Maxthon	1.2	All	All	All

Application	Maxthon	Maxthon	1.2.1	All	All	All

Vendor Declared Affected Products

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

References

Reference	Source	Link
Secunia - Advisories - Maxthon Security ID Disclosure Vulnerability	af854a3a-2127-422b-91ae-364da2661108	secunia.co
www.raffon.net/advisories/maxthon/multvulns.html	af854a3a-2127-422b-91ae-364da2661108	www.raffor
Maxthon Web Browser Plug-in API Security ID Information Disclosure Vulnerability	af854a3a-2127-422b-91ae-364da2661108	www.secur
www.osvdb.org/15424	af854a3a-2127-422b-91ae-364da2661108	www.osvdb
CVE Program record	CVE.ORG	www.cve.o
NVD vulnerability detail	NVD	nvd.nist.go

No vendor comments have been submitted for this CVE.

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