



CVE-2005-0905

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

Summary

CVE	CVE-2005-0905
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 allows remote malicious web sites to obtain potentially sensitive data from the search bar via the m2_search

Risk And Classification

Primary CVSS: v2.0 2.6 from nvd@nist.gov

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

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

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

High

Authentication

None

Confidentiality

Partial

Integrity

None

Availability

None

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Maxthon	Maxthon	1.2	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
404 Not Found			af854a3a-2127-422b-91ae-364da2661108	forum.n
'[Full-disclosure] Maxthon browser search bar information disclosure' - MARC			af854a3a-2127-422b-91ae-364da2661108	marc.in
Secunia - Advisories - Maxthon "m2_search_text" Search Bar Exposure of Information			af854a3a-2127-422b-91ae-364da2661108	secunia
Maxthon Web Browser Search Bar Information Disclosure Vulnerability			af854a3a-2127-422b-91ae-364da2661108	www.se
www.raffon.net/advisories/maxthon/searchbarid.html			af854a3a-2127-422b-91ae-364da2661108	www.ra
CVE Program record			CVE.ORG	www.cv
NVD vulnerability detail			NVD	nvd.nis
No vendor comments have been submitted for this CVE.				
There are currently no legacy QID mappings associated with this CVE.				