CVE-2002-1126

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

Summary

CVE	CVE-2002-1126
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2002-09-24 04:00:00 UTC
Updated	2025-04-03 01:03:51 UTC
Description	Mozilla 1.1 and earlier, and Mozilla-based browsers such as Netscape and Galeon, set the document referrer too quickly in

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	Galeon	Galeon Browser	1.2.4	All	All	All

Application	Galeon	Galeon Browser	1.2.5	All	All	All
Application	Galeon	Galeon Browser	1.2.6	All	All	All
Application	Mozilla	Mozilla	0.9.3	All	All	All
Application	Mozilla	Mozilla	0.9.4	All	All	All
Application	Mozilla	Mozilla	0.9.5	All	All	All
Application	Mozilla	Mozilla	0.9.6	All	All	All
Application	Mozilla	Mozilla	0.9.7	All	All	All
Application	Mozilla	Mozilla	0.9.8	All	All	All
Application	Mozilla	Mozilla	0.9.9	All	All	All
Application	Mozilla	Mozilla	1.0.1	All	All	All
Application	Mozilla	Mozilla	1.1	All	All	All

Vendor Declared Affected Products

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

References

Reference
'Privacy leak in mozilla' - MARC
redhat.com | Red Hat Support
ISS X-Force Database: mozilla-onunload-url-leak (10084): Mozilla "onunload" handler leaks URLs of Web pages
redhat.com | Red Hat Support
Mandrakesoft Security Advisories
145579 – (future_referer) Website can see url of page visited after it (document referer used when loading images with javascript is incorrect v
Mozilla OnUnload Referer Information Leakage 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.

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**