CVE-2008-0826

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

Summary

CVE	CVE-2008-0826
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2008-02-19 20:44:00 UTC
Updated	2026-04-23 00:35:47 UTC
Description	Cross-site scripting (XSS) vulnerability in Claroline before 1.8.9 allows remote attackers to inject arbitrary web script or HTM

Risk And Classification

Primary CVSS: v2.0 4.3 from nvd@nist.gov

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

Problem Types: CWE-79 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

None

Confidentiality

None

Integrity

Partial

Availability

None

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Caroline	Caroline	All	All	All	All

Application	Caroline	Caroline	All	All	All	All
Application	Caroline	Caroline	All	All	All	All
Application	Caroline	Caroline	All	All	All	All
Application	Caroline	Caroline	All	All	All	All
Application	Caroline	Caroline	All	All	All	All
Application	Caroline	Caroline	All	All	All	All
Application	Caroline	Caroline	All	All	All	All

Vendor Declared Affected Products

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

References

Reference	Source
SourceForge.net: Claroline: Files	af854a3a-2127-422b-91ae-364da2661108
Claroline Multiple Remote Vulnerabilities	af854a3a-2127-422b-91ae-364da2661108
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	af854a3a-2127-422b-91ae-364da2661108
Claroline Multiple Vulnerabilities - Secunia Advisories - Vulnerability Intelligence - Secunia.com	af854a3a-2127-422b-91ae-364da2661108
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

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