CVE-2013-4507

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

Summary

CVE	CVE-2013-4507
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2013-11-20 13:19:41 UTC
Updated	2026-04-29 01:13:23 UTC
Description	Cross-site scripting (XSS) vulnerability in CollectiveAccess Providence and Pawtucket before 1.3.1 allows remote attackers

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

EPSS: 0.002630000 probability, percentile 0.496290000 (date 2026-04-29)

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	Collectiveaccess	Pawtucket	1.1	All	All	All
Application	Collectiveaccess	Pawtucket	1.2	All	All	All
Application	Collectiveaccess	Pawtucket	All	All	All	All
Application	Collectiveaccess	Providence	1.1	All	All	All
Application	Collectiveaccess	Providence	1.2	All	All	All
Application	Collectiveaccess	Providence	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
collectiveaccess.org | CollectiveAccess	af854a3a-2
Security Advisory SA55481 - CollectiveAccess Providence / Pawtucket Components Cross-Site Scripting Vulnerability - Secunia	af854a3a-2
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.