



CVE-2005-2624

Published on: 08/19/2005 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:28 PM UTC

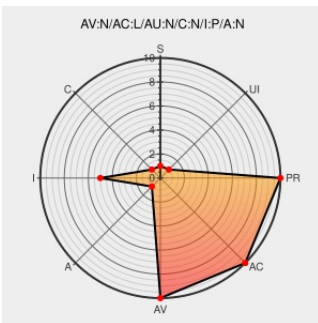
CVE-2005-2624

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



Certain versions of [Cpaint](#) from [Cpaint](#) contain the following vulnerability:

Eval injection vulnerability in CPAINT 1.3-SP allows remote attackers to execute arbitrary ASP code via the `cpaint_argument[]` parameter to (1) `calculator.asp` or (2) `cpaintfile.asp`, which is directly fed into an eval statement.

CVE-2005-2624 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **5 - MEDIUM**

Access
Vector

NETWORK

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

NONE

Integrity
Impact

PARTIAL

Availability
Impact

NONE

CVE References

Description

Tags

Link

'RE: Vulnerability found in CPAINT Ajax Toolkit' - MARC

[marc.info](#)
[text/html](#)

[BUGTRAQ 20050816 RE: Vulnerability found in CPAINT Ajax Toolkit](#)

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type

Vendor

Product

Version

Update

Edition

Language

Application	Cpaint	Cpaint	1.3_sp	All	All	All
Application	Cpaint	Cpaint	1.3_sp	All	All	All
cpe:2.3:a:cpaint:cpaint:1.3_sp:*****:						
cpe:2.3:a:cpaint:cpaint:1.3_sp:*****:						
No vendor comments have been submitted for this CVE						
← Previous ID				Next ID→		