

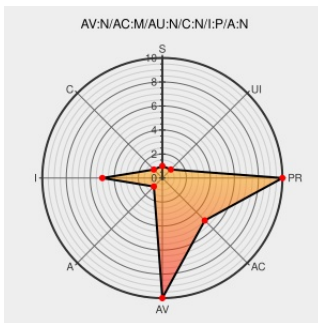


CVE-2006-0650

Published on: 02/13/2006 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:07 PM UTC

CVE-2006-0650

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

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

Cross-site scripting (XSS) vulnerability in cpaint2.inc.php in the CPAINT library before 2.0.3, as used in multiple scripts, allows remote attackers to inject arbitrary web script or HTML via the cpaint_response_type parameter, which is displayed in a resulting error message, as demonstrated using a hex-encoded IFRAME tag.

CVE-2006-0650 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **4.3 - MEDIUM**

Access
Vector

NETWORK

Access
Complexity

MEDIUM

Authentication

NONE

Confidentiality
Impact

NONE

Integrity
Impact

PARTIAL

Availability
Impact

NONE

CVE References

Description

Tags

Link

Contact Support

[Exploit](#)
[Patch](#)
[Vendor Advisory](#)
[www.gulftech.org](#)
[text/html](#)

[MISC](#) [www.gulftech.org/?node=research&article_id=00097-02092006](#)

booleansystems.com

[Exploit](#)
[web.archive.org](#)
[text/html](#)
[Inactive Link](#) [Not Archived](#)

[CONFIRM](#) [cpaint.booleansystems.com/forums/viewtopic.php?t=98](#)

IBM X-Force Exchange

[exchange.xforce.ibmcloud.com](#)
[text/html](#)

[XF](#) [cpaint-response-type-xss\(24594\)](#)

SecurityFocus

[www.securityfocus.com](#)

[BUGTRAQ](#) [20060210 CPAINT AJAX Library](#)

[text/html](#)[Cross Site Scripting](#)

CPAINT AJAX "cpaint_response_type" Cross-Site Scripting - Advisories - Secunia

[Exploit](#)[Patch](#)[Vendor Advisory](#)[web.archive.org](#)[text/html](#)[X SECUNIA 18765](#)

SecurityTracker.com Archives - CPAINT Input Validation Hole in 'cpaint2.inc.php' Permits Cross-Site Scripting Attacks

[securitytracker.com](#)[text/html](#)[SECTrack 1015608](#)

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

[www.vupen.com](#)[text/html](#)[VUPEN ADV-2006-0487](#)

CPAINT TYPE.PHP Cross-Site Scripting Vulnerability

[cve.report \(archive\)](#)[text/html](#)[BID 16559](#)

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	1.0	All	All	All
Application	Cpaint	Cpaint	1.01	All	All	All
Application	Cpaint	Cpaint	1.2	All	All	All
Application	Cpaint	Cpaint	1.3	All	All	All
Application	Cpaint	Cpaint	1.3_sp	All	All	All
Application	Cpaint	Cpaint	1.3_sp1	All	All	All
Application	Cpaint	Cpaint	2.0.0	All	All	All
Application	Cpaint	Cpaint	2.0.1	All	All	All
Application	Cpaint	Cpaint	2.0.2	All	All	All
Application	Cpaint	Cpaint	pre1.0	All	All	All
Application	Cpaint	Cpaint	1.0	All	All	All
Application	Cpaint	Cpaint	1.01	All	All	All
Application	Cpaint	Cpaint	1.2	All	All	All
Application	Cpaint	Cpaint	1.3	All	All	All
Application	Cpaint	Cpaint	1.3_sp	All	All	All
Application	Cpaint	Cpaint	1.3_sp1	All	All	All
Application	Cpaint	Cpaint	2.0.0	All	All	All
Application	Cpaint	Cpaint	2.0.1	All	All	All
Application	Cpaint	Cpaint	2.0.2	All	All	All

Application	Cpaint	Cpaint	2.0.2	All	All	All
Application	Cpaint	Cpaint	pre1.0	All	All	All
cpe:2.3:a:cpaint:cpaint:1.0:*****:						
cpe:2.3:a:cpaint:cpaint:1.01:*****:						
cpe:2.3:a:cpaint:cpaint:1.2:*****:						
cpe:2.3:a:cpaint:cpaint:1.3:*****:						
cpe:2.3:a:cpaint:cpaint:1.3_sp:*****:						
cpe:2.3:a:cpaint:cpaint:1.3_sp1:*****:						
cpe:2.3:a:cpaint:cpaint:2.0.0:*****:						
cpe:2.3:a:cpaint:cpaint:2.0.1:*****:						
cpe:2.3:a:cpaint:cpaint:2.0.2:*****:						
cpe:2.3:a:cpaint:cpaint:pre1.0:*****:						
cpe:2.3:a:cpaint:cpaint:1.0:*****:						
cpe:2.3:a:cpaint:cpaint:1.01:*****:						
cpe:2.3:a:cpaint:cpaint:1.2:*****:						
cpe:2.3:a:cpaint:cpaint:1.3:*****:						
cpe:2.3:a:cpaint:cpaint:1.3_sp:*****:						
cpe:2.3:a:cpaint:cpaint:1.3_sp1:*****:						
cpe:2.3:a:cpaint:cpaint:2.0.0:*****:						
cpe:2.3:a:cpaint:cpaint:2.0.1:*****:						
cpe:2.3:a:cpaint:cpaint:2.0.2:*****:						
cpe:2.3:a:cpaint:cpaint:pre1.0:*****:						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

[site](#). This site includes MITRE data granted under the following [license](#).

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