



CVE-2010-2615

Published on: 07/01/2010 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:09 PM UTC

CVE-2010-2615

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

Certain versions of [Grafik Cms](#) from [Grafik-power](#) contain the following vulnerability:

Multiple cross-site scripting (XSS) vulnerabilities in admin/admin.php in Grafik CMS 1.1.2, and possibly earlier, allow remote attackers to inject arbitrary web script or HTML via the (1) page_menu and (2) description parameters in an edit_page action.

CVE-2010-2615 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

High-Tech Bridge SA - Advisories - XSS vulnerability in Grafik CMS

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

[MISC](#)
[www.htbridge.ch/advisory/xss_vulnerability_in_grafik_cms.html](#)

SecurityFocus

[www.securityfocus.com](#)
[text/html](#)

[BUGTRAQ 20100629 XSS vulnerability in Grafik CMS](#)

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

[Vendor Advisory](#)
[www.vupen.com](#)
[text/html](#)

[VUPEN ADV-2010-1629](#)

High-Tech Bridge SA - Advisories - XSS vulnerability in Grafik CMS

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

[MISC](#)
[www.htbridge.ch/advisory/xss_vulnerability_in_grafik_cms_1.html](#)

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	Grafik-power	Grafik Cms	1.1.1	All	All	All
Application	Grafik-power	Grafik Cms	1.1.1	All	All	All
Application	Grafik-power	Grafik Cms	All	All	All	All
cpe:2.3:a:grafik-power:grafik_cms:1.1.1:*:*:*:*:*:						
cpe:2.3:a:grafik-power:grafik_cms:1.1.1:*:*:*:*:*:						
cpe:2.3:a:grafik-power:grafik_cms:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)