



CVE-2006-1888

Published on: 04/20/2006 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:00 PM UTC

CVE-2006-1888

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



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

phpGraphy 0.9.11 and earlier allows remote attackers to bypass authentication and gain administrator privileges via a direct request to index.php with the editwelcome parameter set to 1, which can then be used to modify the main page to inject arbitrary HTML and web script.

NOTE: XSS attacks are resultant from this issue, since normal

functionality allows the admin to modify pages.

CVE-2006-1888 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **6.8 - MEDIUM**

**Access
Vector**

NETWORK

**Access
Complexity**

MEDIUM

Authentication

NONE

**Confidentiality
Impact**

PARTIAL

**Integrity
Impact**

PARTIAL

**Availability
Impact**

PARTIAL

CVE References

Description

Tags

Link

SecurityTracker.com Archives - phpGraphy 'editwelcome' Function Grants Remote Users Access to Some Administrative Functions

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

[SECTRAK 1015971](#)

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

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

[VUPEN ADV-2006-1379](#)

SecurityFocus

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

[BUGTRAQ 20060417 - PHPGraphy <= 0.9.11 "editwelcome" unauthorized access / cross site scripting -](#)

SecurityFocus

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

[BUGTRAQ 20060418 Re: - PHPGraphy <= 0.9.11 "editwelcome" unauthorized access /](#)

	text/html	CVE-2017-16696 - Unauthorized Access, cross site scripting -
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF phpgraphy-index-xss(25892)
Error 404 :(	Exploit retrogod.altervista.org text/plain Inactive Link Not Archived	MISC retrogod.altervista.org/phpgraphy_0911_adv.html
PHPgraphy Index.PHP Unauthorized Access Vulnerability	Exploit Patch cve.report (archive) text/html	BID 17567
Secunia - Advisories - phpGgraphy "editwelcome" Authentication Bypass	Patch Vendor Advisory web.archive.org text/html	SECUNIA 19705
SecurityReason	securityreason.com text/html	SREASON 733

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	Phpgraphy	Phpgraphy	0.9.10	All	All	All
Application	Phpgraphy	Phpgraphy	0.9.9a	All	All	All
Application	Phpgraphy	Phpgraphy	All	All	All	All
Application	Phpgraphy	Phpgraphy	0.9.10	All	All	All
Application	Phpgraphy	Phpgraphy	0.9.9a	All	All	All
cpe:2.3:a:phpgraphy:phpgraphy:0.9.10:*:*:*:*:*:						
cpe:2.3:a:phpgraphy:phpgraphy:0.9.9a:*:*:*:*:*:						
cpe:2.3:a:phpgraphy:phpgraphy:*:*:*:*:*:						
cpe:2.3:a:phpgraphy:phpgraphy:0.9.10:*:*:*:*:*:						
cpe:2.3:a:phpgraphy:phpgraphy:0.9.9a:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

© [CVE.report](#) 2023   |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)