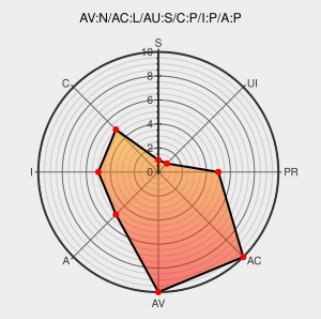
CVE-2004-2538

Published on: 12/31/2004 05:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:13 PM UTC

CVE-2004-2538

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Phpcodegenie from Nilesh Dosooye contain the following vulnerability:

Direct static code injection vulnerability in the PCG simple application generation in phpCodeGenie before 3.0.2 allows remote authenticated users to execute arbitrary code via the (1) header or (2) footer.

CVE-2004-2538 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 6.5 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
SecurityTracker.com Archives - phpCodeGenie Lets Remote Authenticated Users Execute Arbitrary Commands on the Target System	Patch, securitytracker.com, text/html	SECTRACK 1011911
IBM X-Force Exchange	exchange.xforce.ibmcloud.com, text/html	XF phpcodegenie-header-footer-command-execution(17848)
Secunia - Advisories - phpCodeGenie "Simple Application Generation" Code Execution Vulnerability	Patch, Vendor Advisory, web.archive.org, text/html	SECUNIA 12853
No Description Provided	www.osvdb.org, Inactive Link, Not Archived	OSVDB 11102

phpCodeGenie PHP Code Injection Vulnerability	Patch cve.report (archive) text/html	BID 11524
Encountered a 404 error	phpcodegenie.sourceforge.net text/plain Inactive Link Not Archived	CONFIRM phpcodegenie.sourceforge.net/phpCodeGenie/docs/ChangeLog.txt

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	Nilesh Dosooye	Phpcodegenie	1.1	All	All	All
Application	Nilesh Dosooye	Phpcodegenie	1.21	All	All	All
Application	Nilesh Dosooye	Phpcodegenie	1.4	All	All	All
Application	Nilesh Dosooye	Phpcodegenie	3.0_alpha	All	All	All
Application	Nilesh Dosooye	Phpcodegenie	3.0_beta	All	All	All
Application	Nilesh Dosooye	Phpcodegenie	1.1	All	All	All
Application	Nilesh Dosooye	Phpcodegenie	1.21	All	All	All
Application	Nilesh Dosooye	Phpcodegenie	1.4	All	All	All
Application	Nilesh Dosooye	Phpcodegenie	3.0_alpha	All	All	All
Application	Nilesh Dosooye	Phpcodegenie	3.0_beta	All	All	All
Application	Nilesh Dosooye	Phpcodegenie	All	All	All	All

cpe:2.3:a:nilesh_dosooye:phpcodegenie:1.1:*:*:*:*:*:*:*:

cpe:2.3:a:nilesh_dosooye:phpcodegenie:1.21:*:*:*:*:*:*:*:

cpe:2.3:a:nilesh_dosooye:phpcodegenie:1.4:*:*:*:*:*:*:*:

cpe:2.3:a:nilesh_dosooye:phpcodegenie:3.0_alpha:*:*:*:*:*:*:*:

cpe:2.3:a:nilesh_dosooye:phpcodegenie:3.0_beta:*:*:*:*:*:*:*:

cpe:2.3:a:nilesh_dosooye:phpcodegenie:1.1:*:*:*:*:*:*:*:

cpe:2.3:a:nilesh_dosooye:phpcodegenie:1.21:*:*:*:*:*:*:*:

cpe:2.3:a:nilesh_dosooye:phpcodegenie:1.4:*:*:*:*:*:*:*:

cpe:2.3:a:nilesh_dosooye:phpcodegenie:3.0_alpha:*:*:*:*:*:*:*:

cpe:2.3:a:nilesh_dosooye:phpcodegenie:3.0_beta:*:*:*:*:*:*:*:

cpe:2.3:a:nilesh_dosooye:phpcodegenie:*:*:*:*:*:*:*:*:

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 registred 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