



CVE-2006-1069

Published on: 03/07/2006 12:00:00 AM UTC

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

CVE-2006-1069

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

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

Unspecified vulnerability in the session handling for Geeklog 1.4.x before 1.4.0sr2, 1.3.11 before 1.3.11sr5, 1.3.9 before 1.3.9sr5, and possibly earlier versions allows attackers to gain privileges as arbitrary users via unknown vectors.

CVE-2006-1069 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **10 - HIGH**

Access
Vector

NETWORK

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

COMPLETE

Integrity
Impact

COMPLETE

Availability
Impact

COMPLETE

CVE References

Description

Tags

Link

Geeklog - Geeklog 1.4.0sr2, 1.3.11sr5, 1.3.9sr5

[Patch](#)
[www.geeklog.net](#)
[text/html](#)

[CONFIRM](#) www.geeklog.net/article.php/geeklog-1.4.0sr2

Webmail : Solution de messagerie professionnelle - OVHcloud-OVH

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

[VUPEN ADV-2006-0851](#)

Geeklog Lib-sessions.PHP Authorization Bypass Vulnerability

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

[BID 17010](#)

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	Geeklog	Geeklog	1.3.11	All	All	All
Application	Geeklog	Geeklog	1.3.11_sr1	All	All	All
Application	Geeklog	Geeklog	1.3.11_sr2	All	All	All
Application	Geeklog	Geeklog	1.3.11_sr3	All	All	All
Application	Geeklog	Geeklog	1.3.11_sr4	All	All	All
Application	Geeklog	Geeklog	1.3.9	All	All	All
Application	Geeklog	Geeklog	1.3.9_sr1	All	All	All
Application	Geeklog	Geeklog	1.3.9_sr2	All	All	All
Application	Geeklog	Geeklog	1.3.9_sr3	All	All	All
Application	Geeklog	Geeklog	1.3.9_sr4	All	All	All
Application	Geeklog	Geeklog	1.4.0	All	All	All
Application	Geeklog	Geeklog	1.4.0_sr1	All	All	All
Application	Geeklog	Geeklog	1.3.11	All	All	All
Application	Geeklog	Geeklog	1.3.11_sr1	All	All	All
Application	Geeklog	Geeklog	1.3.11_sr2	All	All	All
Application	Geeklog	Geeklog	1.3.11_sr3	All	All	All
Application	Geeklog	Geeklog	1.3.11_sr4	All	All	All
Application	Geeklog	Geeklog	1.3.9	All	All	All
Application	Geeklog	Geeklog	1.3.9_sr1	All	All	All
Application	Geeklog	Geeklog	1.3.9_sr2	All	All	All
Application	Geeklog	Geeklog	1.3.9_sr3	All	All	All
Application	Geeklog	Geeklog	1.3.9_sr4	All	All	All
Application	Geeklog	Geeklog	1.4.0	All	All	All
Application	Geeklog	Geeklog	1.4.0_sr1	All	All	All
cpe:2.3:a:geeklog:geeklog:1.3.11:*:*:*:*:*:						
cpe:2.3:a:geeklog:geeklog:1.3.11_sr1:*:*:*:*:*:						
cpe:2.3:a:geeklog:geeklog:1.3.11_sr2:*:*:*:*:*:						
cpe:2.3:a:geeklog:geeklog:1.3.11_sr3:*:*:*:*:*:						
cpe:2.3:a:geeklog:geeklog:1.3.11_sr4:*:*:*:*:*:						
cpe:2.3:a:geeklog:geeklog:1.3.9:*:*:*:*:*:						

cpe:2.3:a:geeklog:geeklog:1.3.9_sr1:*****:
cpe:2.3:a:geeklog:geeklog:1.3.9_sr2:*****:
cpe:2.3:a:geeklog:geeklog:1.3.9_sr3:*****:
cpe:2.3:a:geeklog:geeklog:1.3.9_sr4:*****:
cpe:2.3:a:geeklog:geeklog:1.4.0:*****:
cpe:2.3:a:geeklog:geeklog:1.4.0_sr1:*****:
cpe:2.3:a:geeklog:geeklog:1.3.11:*****:
cpe:2.3:a:geeklog:geeklog:1.3.11_sr1:*****:
cpe:2.3:a:geeklog:geeklog:1.3.11_sr2:*****:
cpe:2.3:a:geeklog:geeklog:1.3.11_sr3:*****:
cpe:2.3:a:geeklog:geeklog:1.3.11_sr4:*****:
cpe:2.3:a:geeklog:geeklog:1.3.9:*****:
cpe:2.3:a:geeklog:geeklog:1.3.9_sr1:*****:
cpe:2.3:a:geeklog:geeklog:1.3.9_sr2:*****:
cpe:2.3:a:geeklog:geeklog:1.3.9_sr3:*****:
cpe:2.3:a:geeklog:geeklog:1.3.9_sr4:*****:
cpe:2.3:a:geeklog:geeklog:1.4.0:*****:
cpe:2.3:a:geeklog:geeklog:1.4.0_sr1:*****:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)