



# CVE-2006-2699

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2006-2699
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2006-05-31 10:06:00 UTC
<b>Updated</b>	2018-10-18 16:41:00 UTC
<b>Description</b>	Cross-site scripting (XSS) vulnerability in getimage.php in Geeklog 1.4.0sr2 and earlier allows remote attackers to inject art

## Risk And Classification

**Problem Types:** NVD-CWE-Other

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Geeklog</a>	<a href="#">Geeklog</a>	1.3	All	All	All
Application	<a href="#">Geeklog</a>	<a href="#">Geeklog</a>	1.3.10	All	All	All
Application	<a href="#">Geeklog</a>	<a href="#">Geeklog</a>	1.3.10_rc1	All	All	All
Application	<a href="#">Geeklog</a>	<a href="#">Geeklog</a>	1.3.10_rc2	All	All	All
Application	<a href="#">Geeklog</a>	<a href="#">Geeklog</a>	1.3.10_rc3	All	All	All
Application	<a href="#">Geeklog</a>	<a href="#">Geeklog</a>	1.3.11	All	All	All
Application	<a href="#">Geeklog</a>	<a href="#">Geeklog</a>	1.3.11_rc1	All	All	All
Application	<a href="#">Geeklog</a>	<a href="#">Geeklog</a>	1.3.11_sr1	All	All	All
Application	<a href="#">Geeklog</a>	<a href="#">Geeklog</a>	1.3.11_sr2	All	All	All
Application	<a href="#">Geeklog</a>	<a href="#">Geeklog</a>	1.3.11_sr3	All	All	All
Application	<a href="#">Geeklog</a>	<a href="#">Geeklog</a>	1.3.11_sr4	All	All	All
Application	<a href="#">Geeklog</a>	<a href="#">Geeklog</a>	1.3.5	All	All	All
Application	<a href="#">Geeklog</a>	<a href="#">Geeklog</a>	1.3.5_sr1	All	All	All
Application	<a href="#">Geeklog</a>	<a href="#">Geeklog</a>	1.3.6	All	All	All
Application	<a href="#">Geeklog</a>	<a href="#">Geeklog</a>	1.3.7	All	All	All
Application	<a href="#">Geeklog</a>	<a href="#">Geeklog</a>	1.3.7_sr1	All	All	All
Application	<a href="#">Geeklog</a>	<a href="#">Geeklog</a>	1.3.7_sr2	All	All	All

Application	<a href="#">Geeklog</a>	<a href="#">Geeklog</a>	1.3.7_sr3	All	All	All
Application	<a href="#">Geeklog</a>	<a href="#">Geeklog</a>	1.3.7_sr4	All	All	All
Application	<a href="#">Geeklog</a>	<a href="#">Geeklog</a>	1.3.7_sr5	All	All	All
Application	<a href="#">Geeklog</a>	<a href="#">Geeklog</a>	1.3.8	All	All	All
Application	<a href="#">Geeklog</a>	<a href="#">Geeklog</a>	1.3.8_1	All	All	All
Application	<a href="#">Geeklog</a>	<a href="#">Geeklog</a>	1.3.8_1_sr1	All	All	All
Application	<a href="#">Geeklog</a>	<a href="#">Geeklog</a>	1.3.8_1_sr2	All	All	All
Application	<a href="#">Geeklog</a>	<a href="#">Geeklog</a>	1.3.8_1_sr3	All	All	All
Application	<a href="#">Geeklog</a>	<a href="#">Geeklog</a>	1.3.8_1_sr4	All	All	All
Application	<a href="#">Geeklog</a>	<a href="#">Geeklog</a>	1.3.8_1_sr5	All	All	All
Application	<a href="#">Geeklog</a>	<a href="#">Geeklog</a>	1.3.8_1_sr6	All	All	All
Application	<a href="#">Geeklog</a>	<a href="#">Geeklog</a>	1.3.9	All	All	All
Application	<a href="#">Geeklog</a>	<a href="#">Geeklog</a>	1.3.9_rc1	All	All	All
Application	<a href="#">Geeklog</a>	<a href="#">Geeklog</a>	1.3.9_rc2	All	All	All
Application	<a href="#">Geeklog</a>	<a href="#">Geeklog</a>	1.3.9_rc3	All	All	All
Application	<a href="#">Geeklog</a>	<a href="#">Geeklog</a>	1.3.9_sr1	All	All	All
Application	<a href="#">Geeklog</a>	<a href="#">Geeklog</a>	1.3.9_sr2	All	All	All
Application	<a href="#">Geeklog</a>	<a href="#">Geeklog</a>	1.3.9_sr3	All	All	All
Application	<a href="#">Geeklog</a>	<a href="#">Geeklog</a>	1.3.9_sr4	All	All	All
Application	<a href="#">Geeklog</a>	<a href="#">Geeklog</a>	1.35	All	All	All
Application	<a href="#">Geeklog</a>	<a href="#">Geeklog</a>	1.4.0	All	All	All
Application	<a href="#">Geeklog</a>	<a href="#">Geeklog</a>	1.4.0_beta1	All	All	All
Application	<a href="#">Geeklog</a>	<a href="#">Geeklog</a>	1.4.0_sr1	All	All	All
Application	<a href="#">Geeklog</a>	<a href="#">Geeklog</a>	1.4.0_sr2	All	All	All
Application	<a href="#">Geeklog</a>	<a href="#">Geeklog</a>	1.3	All	All	All
Application	<a href="#">Geeklog</a>	<a href="#">Geeklog</a>	1.3.10	All	All	All
Application	<a href="#">Geeklog</a>	<a href="#">Geeklog</a>	1.3.10_rc1	All	All	All
Application	<a href="#">Geeklog</a>	<a href="#">Geeklog</a>	1.3.10_rc2	All	All	All
Application	<a href="#">Geeklog</a>	<a href="#">Geeklog</a>	1.3.10_rc3	All	All	All
Application	<a href="#">Geeklog</a>	<a href="#">Geeklog</a>	1.3.11	All	All	All
Application	<a href="#">Geeklog</a>	<a href="#">Geeklog</a>	1.3.11_rc1	All	All	All
Application	<a href="#">Geeklog</a>	<a href="#">Geeklog</a>	1.3.11_sr1	All	All	All
Application	<a href="#">Geeklog</a>	<a href="#">Geeklog</a>	1.3.11_sr2	All	All	All
Application	<a href="#">Geeklog</a>	<a href="#">Geeklog</a>	1.3.11_sr3	All	All	All
Application	<a href="#">Geeklog</a>	<a href="#">Geeklog</a>	1.3.11_sr4	All	All	All

Application	<a href="#">Geeklog</a>	<a href="#">Geeklog</a>	1.3.5	All	All	All
Application	<a href="#">Geeklog</a>	<a href="#">Geeklog</a>	1.3.5_sr1	All	All	All
Application	<a href="#">Geeklog</a>	<a href="#">Geeklog</a>	1.3.6	All	All	All
Application	<a href="#">Geeklog</a>	<a href="#">Geeklog</a>	1.3.7	All	All	All
Application	<a href="#">Geeklog</a>	<a href="#">Geeklog</a>	1.3.7_sr1	All	All	All
Application	<a href="#">Geeklog</a>	<a href="#">Geeklog</a>	1.3.7_sr2	All	All	All
Application	<a href="#">Geeklog</a>	<a href="#">Geeklog</a>	1.3.7_sr3	All	All	All
Application	<a href="#">Geeklog</a>	<a href="#">Geeklog</a>	1.3.7_sr4	All	All	All
Application	<a href="#">Geeklog</a>	<a href="#">Geeklog</a>	1.3.7_sr5	All	All	All
Application	<a href="#">Geeklog</a>	<a href="#">Geeklog</a>	1.3.8	All	All	All
Application	<a href="#">Geeklog</a>	<a href="#">Geeklog</a>	1.3.8_1	All	All	All
Application	<a href="#">Geeklog</a>	<a href="#">Geeklog</a>	1.3.8_1_sr1	All	All	All
Application	<a href="#">Geeklog</a>	<a href="#">Geeklog</a>	1.3.8_1_sr2	All	All	All
Application	<a href="#">Geeklog</a>	<a href="#">Geeklog</a>	1.3.8_1_sr3	All	All	All
Application	<a href="#">Geeklog</a>	<a href="#">Geeklog</a>	1.3.8_1_sr4	All	All	All
Application	<a href="#">Geeklog</a>	<a href="#">Geeklog</a>	1.3.8_1_sr5	All	All	All
Application	<a href="#">Geeklog</a>	<a href="#">Geeklog</a>	1.3.8_1_sr6	All	All	All
Application	<a href="#">Geeklog</a>	<a href="#">Geeklog</a>	1.3.9	All	All	All
Application	<a href="#">Geeklog</a>	<a href="#">Geeklog</a>	1.3.9_rc1	All	All	All
Application	<a href="#">Geeklog</a>	<a href="#">Geeklog</a>	1.3.9_rc2	All	All	All
Application	<a href="#">Geeklog</a>	<a href="#">Geeklog</a>	1.3.9_rc3	All	All	All
Application	<a href="#">Geeklog</a>	<a href="#">Geeklog</a>	1.3.9_sr1	All	All	All
Application	<a href="#">Geeklog</a>	<a href="#">Geeklog</a>	1.3.9_sr2	All	All	All
Application	<a href="#">Geeklog</a>	<a href="#">Geeklog</a>	1.3.9_sr3	All	All	All
Application	<a href="#">Geeklog</a>	<a href="#">Geeklog</a>	1.3.9_sr4	All	All	All
Application	<a href="#">Geeklog</a>	<a href="#">Geeklog</a>	1.35	All	All	All
Application	<a href="#">Geeklog</a>	<a href="#">Geeklog</a>	1.4.0	All	All	All
Application	<a href="#">Geeklog</a>	<a href="#">Geeklog</a>	1.4.0_beta1	All	All	All
Application	<a href="#">Geeklog</a>	<a href="#">Geeklog</a>	1.4.0_sr1	All	All	All
Application	<a href="#">Geeklog</a>	<a href="#">Geeklog</a>	1.4.0_sr2	All	All	All

## References

Reference	Source	Link	Tags
IBM X-Force Exchange	XF	<a href="https://exchange.xforce.ibmcloud.com">exchange.xforce.ibmcloud.com</a>	
SecurityFocus	BUGTRAQ	<a href="http://www.securityfocus.com">www.securityfocus.com</a>	
geeklog multiple vulnerabilities - CXSecurity.com	SREASON	<a href="https://securityreason.com">securityreason.com</a>	

KAPDA :: Geeklog multiple vulnerabilities	MISC	<a href="http://kapda.ir">kapda.ir</a>	Exploit, Patch, Ven
Geeklog - Security	CONFIRM	<a href="http://www.geeklog.net">www.geeklog.net</a>	Patch
Geeklog Multiple Input Validation Vulnerabilities	BID	<a href="http://www.securityfocus.com">www.securityfocus.com</a>	Exploit, Patch
Geeklog Multiple Vulnerabilities and Weaknesses - Advisories - Secunia	SECUNIA	<a href="http://secunia.com">secunia.com</a>	Exploit, Patch, Ven
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	<a href="http://www.vupen.com">www.vupen.com</a>	
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>	canonical, analysis

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](http://CVE.report) 2026 |

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](http://The MITRE Corporation) and the authoritative source of CVE content is [MITRE's CVE web site](http://MITRE's CVE web site). This site includes MITRE data granted under the following [license](http://license).

**Free CVE JSON API** [cve.report/api](http://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](http://status.cve.report)