



CVE-2006-3884

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

Summary

CVE	CVE-2006-3884
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2006-07-27 01:04:00 UTC
Updated	2018-10-17 21:32:00 UTC
Description	Multiple SQL injection vulnerabilities in links.php in Gonafish LinksCaffe 3.0 allow remote attackers to execute arbitrary SQL

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Gonafish	Linkscaffe	3.0	All	All	All
Application	Gonafish	Linkscaffe	3.0	All	All	All

References

Reference	Source
SecurityTracker.com Archives - LinksCaffe Input Validation Holes Permits Cross-Site Scripting, SQL Injection, and Command Execution	SECT
IBM X-Force Exchange	XF
IBM X-Force Exchange	XF
SecurityReason - LinksCaffe 3.0 SQL injection/Command Execution Vulnerabilities	SR
27518	OS
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VU
LinksCaffe Multiple Input Validation Vulnerabilities	BID
LinksCaffe Cross-Site Scripting and SQL Injection - Advisories - Secunia	SECT
SecurityFocus	BU
CVE Program record	CV
NVD vulnerability detail	NV

No vendor comments have been submitted for this CVE.

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

© [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](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API [cve.report/api](#)

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