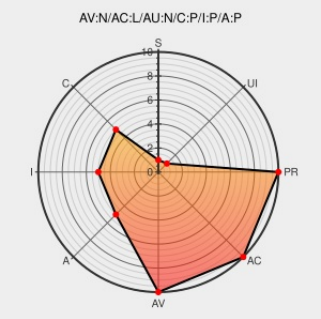
CVE-2006-1706

Published on: 04/11/2006 12:00:00 AM UTC

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

CVE-2006-1706

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



Certain versions of Shopweezle from Kansok Communications contain the following vulnerability:

Multiple SQL injection vulnerabilities in Shopweezle 2.0 allow remote attackers to execute arbitrary SQL commands via the (1) itemID parameter to (a) login.php and (b) memo.php; and the (2) itemgr, (3) brandID, and (4) album parameters to (c) index.php. NOTE: this issue also produces resultant full path disclosure from invalid SQL queries.

CVE-2006-1706 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 7.5 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	www.vupen.com text/html	VUPEN ADV-2006-1291
No Description Provided	www.osvdb.org Inactive Link Not Archived	OSVDB 24473
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF shopweezle-multiple-sql-injection(25723)
- UNSECURED SYSTEMS -: Shopweezle 2.0 multiple vuln.	pridels0.blogspot.com text/html	MISC pridels0.blogspot.com/2006/04/shopweezle-20-multiple-vuln.html
No Description Provided	www.osvdb.org	OSVDB 24471

	Inactive Link Not Archived	
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF shopweezle-multiple-path-disclosure(25724)
Secunia - Advisories - Shopweezle Multiple SQL Injection Vulnerabilities	Vendor Advisory web.archive.org text/html	SECUNIA 19593
ShopWeezle Multiple SQL Injection Vulnerabilities	Exploit cve.report (archive) text/html	BID 17441
No Description Provided	www.osvdb.org Inactive Link Not Archived	OSVDB 24472
No Description Provided	www.osvdb.org Inactive Link Not Archived	OSVDB 24470

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Kansok Communications	Shopweezle	2.0	All	All	All
Application	Kansok Communications	Shopweezle	2.0_personal	All	All	All
Application	Kansok Communications	Shopweezle	2.0_professional	All	All	All
Application	Kansok Communications	Shopweezle	2.0_professional_plus	All	All	All
Application	Kansok Communications	Shopweezle	2.0	All	All	All
Application	Kansok Communications	Shopweezle	2.0_personal	All	All	All
Application	Kansok Communications	Shopweezle	2.0_professional	All	All	All
Application	Kansok Communications	Shopweezle	2.0_professional_plus	All	All	All

cpe:2.3:a:kansok_communications:shopweezle:2.0:*:*:*:*:*:*:*:

cpe:2.3:a:kansok_communications:shopweezle:2.0_personal:*:*:*:*:*:*:*:

cpe:2.3:a:kansok_communications:shopweezle:2.0_professional:*:*:*:*:*:*:*:

cpe:2.3:a:kansok_communications:shopweezle:2.0_professional_plus:*:*:*:*:*:*:*:

cpe:2.3:a:kansok_communications:shopweezle:2.0:*:*:*:*:*:*:*:

cpe:2.3:a:kansok_communications:shopweezle:2.0_personal:*:*:*:*:*:*:*:

cpe:2.3:a:kansok_communications:shopweezle:2.0_professional:*:*:*:*:*:*:*:

cpe:2.3:a:kansok_communications:shopweezle:2.0_professional_plus:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→