



# CVE-2004-2695

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2004-2695
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2004-12-31 05:00:00 UTC
<b>Updated</b>	2020-02-24 15:55:00 UTC
<b>Description</b>	SQL injection vulnerability in the Authorize.net callback code (subscriptions/authorize.php) in Jelsoft vBulletin 3.0 through 3

## Risk And Classification

**Problem Types:** CWE-89

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Jelsoft	Vbulletin	3.0	All	All	All
Application	Jelsoft	Vbulletin	3.0.1	All	All	All
Application	Jelsoft	Vbulletin	3.0.2	All	All	All
Application	Jelsoft	Vbulletin	3.0.3	All	All	All
Application	Jelsoft	Vbulletin	3.0_beta_2	All	All	All
Application	Jelsoft	Vbulletin	3.0_beta_3	All	All	All
Application	Jelsoft	Vbulletin	3.0_beta_4	All	All	All
Application	Jelsoft	Vbulletin	3.0_beta_5	All	All	All
Application	Jelsoft	Vbulletin	3.0_beta_6	All	All	All
Application	Jelsoft	Vbulletin	3.0_beta_7	All	All	All
Application	Jelsoft	Vbulletin	3.0_gamma	All	All	All
Application	Jelsoft	Vbulletin	3.0	All	All	All
Application	Jelsoft	Vbulletin	3.0.1	All	All	All
Application	Jelsoft	Vbulletin	3.0.2	All	All	All
Application	Jelsoft	Vbulletin	3.0.3	All	All	All
Application	Jelsoft	Vbulletin	3.0_beta_2	All	All	All
Application	Jelsoft	Vbulletin	3.0_beta_3	All	All	All

Application	<a href="#">Jelsoft</a>	<a href="#">Vbulletin</a>	3.0_beta_4	All	All	All
Application	<a href="#">Jelsoft</a>	<a href="#">Vbulletin</a>	3.0_beta_5	All	All	All
Application	<a href="#">Jelsoft</a>	<a href="#">Vbulletin</a>	3.0_beta_6	All	All	All
Application	<a href="#">Jelsoft</a>	<a href="#">Vbulletin</a>	3.0_beta_7	All	All	All
Application	<a href="#">Jelsoft</a>	<a href="#">Vbulletin</a>	3.0_gamma	All	All	All
Application	<a href="#">Point-to-point Protocol Project</a>	<a href="#">Point-to-point Protocol</a>	2.4.1	All	All	All
Application	<a href="#">Point-to-point Protocol Project</a>	<a href="#">Point-to-point Protocol</a>	2.4.1	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>	
vBulletin > Bug: SQL Injection Attacks - Reported by Secunia.com	CONFIRM	<a href="https://www.vbulletin.com">www.vbulletin.com</a>	Patch
vBulletin 3.0.4 Released - vBulletin Community Forum	CONFIRM	<a href="https://www.vbulletin.com">www.vbulletin.com</a>	
vBulletin SQL Injection Vulnerability	BID	<a href="https://www.securityfocus.com">www.securityfocus.com</a>	
SecuriTeam.com (vBulletin SQL Injection While Verifying Subscription Information)	MISC	<a href="https://www.securiteam.com">www.securiteam.com</a>	
Secunia - Advisories - vBulletin "x_invoice_num" SQL Injection Vulnerability	SECUNIA	<a href="https://secunia.com">secunia.com</a>	Vendor /
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonica
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonica

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](#).

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