



CVE-2006-1384

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

Summary

CVE	CVE-2006-1384
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2006-03-24 11:02:00 UTC
Updated	2017-07-20 01:30:00 UTC
Description	Cross-site scripting (XSS) vulnerability in apwc_win_main.jsp in the web console in IBM Tivoli Business Systems Manager (TBSM) 3.1.0 allows an attacker to execute arbitrary JavaScript code via a crafted request to the /apwc/win/main.jsp endpoint. This vulnerability is present in TBSM 3.1.0 through 3.1.1.0. The vulnerability is caused by insufficient validation of the 'skin' parameter value, which is used to render the web console. An attacker can exploit this by sending a request with a malicious 'skin' parameter value, which will be executed as JavaScript code in the browser. The impact is that an attacker can execute arbitrary code and potentially compromise the confidentiality and integrity of the system.

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Ibm	Tivoli Business Systems Manager	3.1	All	All	All
Application	Ibm	Tivoli Business Systems Manager	3.1	All	All	All

References

Reference

IBM X-Force Exchange
IBM Tivoli Business Systems Manager Input Validation Flaw in 'apwc_win_main.jsp' Permits Cross-Site Scripting Attacks - SecurityTracker
IBM Tivoli Business Systems Manager Cross-Site Scripting - Advisories - Secunia
IBM OA14904: INSUFFICIENT VALIDATION OF THE SKIN PARAMETER VALUE LEADING TO A TBSM CROSS-SITE SCRIPTING VULNERABILITY
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH
IBM Tivoli Business Systems Manager APWC_Win_Main.JSP Cross-Site Scripting Vulnerability
24069
CVE Program record
NVD vulnerability detail

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](#)