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 (

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 VULNE
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.

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**