



CVE-2004-2086

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

Summary

CVE	CVE-2004-2086
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2004-02-06 05:00:00 UTC
Updated	2017-07-11 01:31:00 UTC
Description	Stack-based buffer overflow in results.stm for Sambar Server before the 6.0 production release allows remote attackers to c

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Sambar	Sambar Server	6.0	All	All	All
Application	Sambar	Sambar Server	6.0	beta3	All	All
Application	Sambar	Sambar Server	6.0	All	All	All
Application	Sambar	Sambar Server	6.0	beta3	All	All

References

Reference	Source	Link
5786	OSVDB	www.osvc
Sambar Server Results.STM Post Request Buffer Overflow Vulnerability	BID	www.secu
Mailing Lists	VULN-DEV	www.secu
Sambar Server Security Alert	CONFIRM	www.sam
IBM X-Force Exchange	XF	exchange
Sambar Server 'results.stm' POST Request Buffer Overflow May Permit Remote Code Execution - SecurityTracker	SECTrack	securitytra
CVE Program record	CVE.ORG	www.cve.
NVD vulnerability detail	NVD	nvd.nist.g

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](#)