



CVE-2003-1286

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

Summary

CVE	CVE-2003-1286
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2003-12-31 05:00:00 UTC
Updated	2017-07-11 01:29:00 UTC
Description	HTTP Proxy in Sambar Server before 6.0 beta 6, when security.ini lacks a 127.0.0.1 proxydeny entry, allows remote attacks

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	5.0	All	All	All
Application	Sambar	Sambar Server	5.0	beta1	All	All
Application	Sambar	Sambar Server	5.0	beta2	All	All
Application	Sambar	Sambar Server	5.0	beta3	All	All
Application	Sambar	Sambar Server	5.0	beta4	All	All
Application	Sambar	Sambar Server	5.0	beta5	All	All
Application	Sambar	Sambar Server	5.0	beta6	All	All
Application	Sambar	Sambar Server	5.1	All	All	All
Application	Sambar	Sambar Server	5.1	beta1	All	All
Application	Sambar	Sambar Server	5.1	beta2	All	All
Application	Sambar	Sambar Server	5.1	beta3	All	All
Application	Sambar	Sambar Server	5.1	beta4	All	All
Application	Sambar	Sambar Server	5.1	beta5	All	All
Application	Sambar	Sambar Server	5.2	All	All	All
Application	Sambar	Sambar Server	5.3	All	All	All
Application	Sambar	Sambar Server	6.0	beta1	All	All
Application	Sambar	Sambar Server	6.0	beta2	All	All

Application	Sambar	Sambar Server	6.0	beta3	All	All
Application	Sambar	Sambar Server	6.0	beta4	All	All
Application	Sambar	Sambar Server	6.0	beta5	All	All
Application	Sambar	Sambar Server	5.0	All	All	All
Application	Sambar	Sambar Server	5.0	beta1	All	All
Application	Sambar	Sambar Server	5.0	beta2	All	All
Application	Sambar	Sambar Server	5.0	beta3	All	All
Application	Sambar	Sambar Server	5.0	beta4	All	All
Application	Sambar	Sambar Server	5.0	beta5	All	All
Application	Sambar	Sambar Server	5.0	beta6	All	All
Application	Sambar	Sambar Server	5.1	All	All	All
Application	Sambar	Sambar Server	5.1	beta1	All	All
Application	Sambar	Sambar Server	5.1	beta2	All	All
Application	Sambar	Sambar Server	5.1	beta3	All	All
Application	Sambar	Sambar Server	5.1	beta4	All	All
Application	Sambar	Sambar Server	5.1	beta5	All	All
Application	Sambar	Sambar Server	5.2	All	All	All
Application	Sambar	Sambar Server	5.3	All	All	All
Application	Sambar	Sambar Server	6.0	beta1	All	All
Application	Sambar	Sambar Server	6.0	beta2	All	All
Application	Sambar	Sambar Server	6.0	beta3	All	All
Application	Sambar	Sambar Server	6.0	beta4	All	All
Application	Sambar	Sambar Server	6.0	beta5	All	All

References						
Reference				Source	Link	
Accenture Let there be change				IDEFENSE	www.iddefense.com	
SecurityTracker.com Archives - Sambar Server Contains Multiple Unspecified Vulnerabilities				SECTrack	securitytracker.com	
20040430 SECURITY.NNOV: Sambar security quest				BUGTRAQ	archives.neohapsis.com	
Secunia - Advisories - Sambar Server Multiple Vulnerabilities				SECUNIA	secunia.com	
Sambar Server Security Alert				CONFIRM	www.sambar.com	
Sambar Open Proxy and Authentication Bypass Vulnerability				BID	www.securityfocus.com	
IBM X-Force Exchange				XF	exchange.xforce.ibmcloud.com	
CVE Program record				CVE.ORG	www.cve.org	
NVD vulnerability detail				NVD	nvd.nist.gov	

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](#)