



CVE-2006-0578

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2006-0578
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2006-02-08 01:02:00 UTC
Updated	2018-10-30 16:25:00 UTC
Description	Blue Coat Proxy Security Gateway OS (SGOS) 4.1.2.1 does not enforce CONNECT rules when using Deep Content Inspection

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Bluecoat	Sgos	4.1.2.1	All	All	All
Operating System	Bluecoat	Sgos	4.1.2.1	All	All	All

References

Reference	Source
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN
IBM X-Force Exchange	XF
SecurityTracker.com Archives - Blue Coat ProxySG Policy Error May Let Remote Users Bypass Default CONNECT Policy Rules	SECTRAC
Blue Coat ProxySG SGOS Two Security Issues - Advisories - Secunia	SECUNIA
Blue Coat Support - Security Advisories	CONFIRM
www.secumind.net/content/french/modules/news/article.php	MISC
22853	OSVDB
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

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](#)