



CVE-2005-4085

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

Summary

CVE	CVE-2005-4085
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2005-12-31 05:00:00 UTC
Updated	2011-03-08 02:27:00 UTC
Description	Buffer overflow in BlueCoat (a) WinProxy before 6.1a and (b) the web console access functionality in ProxyAV before 2.4.2

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Bluecoat	Proxyav	All	All	All	All
Hardware	Bluecoat	Proxyav	All	All	All	All
Application	Bluecoat	Webproxy	4.0	r1a	All	All
Application	Bluecoat	Webproxy	4.0	r1b	All	All
Application	Bluecoat	Webproxy	4.0	r1c	All	All
Application	Bluecoat	Webproxy	4.0	r1e	All	All
Application	Bluecoat	Webproxy	4.0	r1f	All	All
Application	Bluecoat	Webproxy	4.0	r1h	All	All
Application	Bluecoat	Webproxy	4.0	r1k	All	All
Application	Bluecoat	Webproxy	4.0	r1m	All	All
Application	Bluecoat	Webproxy	4.0	r1n	All	All
Application	Bluecoat	Webproxy	4.0	r1p	All	All
Application	Bluecoat	Webproxy	5.0	r1a	All	All
Application	Bluecoat	Webproxy	5.0	r1b	All	All
Application	Bluecoat	Webproxy	5.0	r1c	All	All
Application	Bluecoat	Webproxy	5.1	r1a	All	All
Application	Bluecoat	Webproxy	5.1	r1d	All	All

Application	Bluecoat	Webproxy	5.1	r1e	All	All
Application	Bluecoat	Webproxy	5.2	r1a	All	All
Application	Bluecoat	Webproxy	6.0	r1a	All	All
Application	Bluecoat	Webproxy	6.0	r1c	All	All
Application	Bluecoat	Webproxy	4.0	r1a	All	All
Application	Bluecoat	Webproxy	4.0	r1b	All	All
Application	Bluecoat	Webproxy	4.0	r1c	All	All
Application	Bluecoat	Webproxy	4.0	r1e	All	All
Application	Bluecoat	Webproxy	4.0	r1f	All	All
Application	Bluecoat	Webproxy	4.0	r1h	All	All
Application	Bluecoat	Webproxy	4.0	r1k	All	All
Application	Bluecoat	Webproxy	4.0	r1m	All	All
Application	Bluecoat	Webproxy	4.0	r1n	All	All
Application	Bluecoat	Webproxy	4.0	r1p	All	All
Application	Bluecoat	Webproxy	5.0	r1a	All	All
Application	Bluecoat	Webproxy	5.0	r1b	All	All
Application	Bluecoat	Webproxy	5.0	r1c	All	All
Application	Bluecoat	Webproxy	5.1	r1a	All	All
Application	Bluecoat	Webproxy	5.1	r1d	All	All
Application	Bluecoat	Webproxy	5.1	r1e	All	All
Application	Bluecoat	Webproxy	5.2	r1a	All	All
Application	Bluecoat	Webproxy	6.0	r1a	All	All
Application	Bluecoat	Webproxy	6.0	r1c	All	All

References

Reference	Source	Link
Secunia - Advisories - Blue Coat ProxyAV Host Header Buffer Overflow Vulnerability	SECUNIA	secunia.com
Blue Coat Systems WinProxy Remote Host Header Buffer Overflow Vulnerability	BID	www.securityfocus.com/bid
Blue Coat WinProxy Host Header Buffer Overflow Lets Remote Users Execute Arbitrary Code - SecurityTracker	SECTRACK	securitytracker.com
Secunia - Advisories - Blue Coat WinProxy Multiple Vulnerabilities	SECUNIA	secunia.com
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	www.vupen.com
Blue Coat Systems - Security Advisories	CONFIRM	www.bluecoat.com
Accenture Let there be change	IDEFENSE	www.idefense.com
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	www.vupen.com
CVE Program record	CVE.ORG	www.cve.org

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](#)