



CVE-2009-5128

Published on: 08/26/2012 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:27 PM UTC

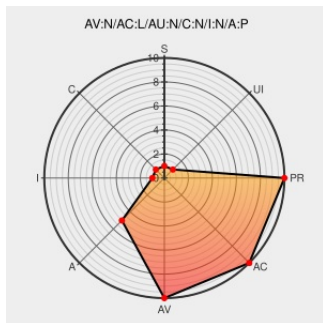
CVE-2009-5128

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



Certain versions of [Websense V10000](#) from [Websense](#) contain the following vulnerability:

The Websense V10000 appliance before 1.0.1 allows remote attackers to cause a denial of service (memory consumption and process crash) via a large file that is not properly handled during buffering.

CVE-2009-5128 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **5 - MEDIUM**

Access Vector

Access Complexity

Authentication

NETWORK

LOW

NONE

Confidentiality Impact

Integrity Impact

Availability Impact

NONE

NONE

PARTIAL

CVE References

Description

Tags

Link

[kb.websense.com
application/pdf](#)



CONFIRM

[kb.websense.com/pf/12/webfiles/V10000%20Documentation/V10000%20Patches/v1.0.1/V10000_v1.0.1_F](#)

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware 	Websense	Websense V10000	1.0.0	All	All	All
Hardware 	Websense	Websense V10000	1.0.0	All	All	All
cpe:2.3:h:websense:websense_v10000:1.0.0:*****:						
cpe:2.3:h:websense:websense_v10000:1.0.0:*****:						
No vendor comments have been submitted for this CVE						
← Previous ID			Next ID→			