



CVE-2016-1383

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

Summary

CVE	CVE-2016-1383
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-05-25 01:59:00 UTC
Updated	2016-12-01 03:05:00 UTC
Description	Memory leak in Cisco AsyncOS through 8.8 on Web Security Appliance (WSA) devices allows remote attackers to cause a

Risk And Classification

Problem Types: CWE-399

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Cisco	Web Security Appliance	-	All	All	All
Hardware	Cisco	Web Security Appliance	-	All	All	All
Application	Cisco	Web Security Appliance Wsa	5.6.0-623	All	All	All
Application	Cisco	Web Security Appliance Wsa	6.0.0-000	All	All	All
Application	Cisco	Web Security Appliance Wsa	7.1.0	All	All	All
Application	Cisco	Web Security Appliance Wsa	7.1.1	All	All	All
Application	Cisco	Web Security Appliance Wsa	7.1.2	All	All	All
Application	Cisco	Web Security Appliance Wsa	7.1.3	All	All	All
Application	Cisco	Web Security Appliance Wsa	7.1.4	All	All	All
Application	Cisco	Web Security Appliance Wsa	7.5.0-000	All	All	All
Application	Cisco	Web Security Appliance Wsa	7.5.0-825	All	All	All
Application	Cisco	Web Security Appliance Wsa	7.5.1-000	All	All	All
Application	Cisco	Web Security Appliance Wsa	7.5.2-000	All	All	All
Application	Cisco	Web Security Appliance Wsa	7.7.0-000	All	All	All
Application	Cisco	Web Security Appliance Wsa	7.7.1-000	All	All	All
Application	Cisco	Web Security Appliance Wsa	8.0.0-000	All	All	All
Application	Cisco	Web Security Appliance Wsa	8.0.5	All	All	All

Application	Cisco	Web Security Appliance Wsa	8.0.6	All	All	All
Application	Cisco	Web Security Appliance Wsa	8.0.6-078	All	All	All
Application	Cisco	Web Security Appliance Wsa	8.0.6-119	All	All	All
Application	Cisco	Web Security Appliance Wsa	8.0.7	All	All	All
Application	Cisco	Web Security Appliance Wsa	8.0.7-142	All	All	All
Application	Cisco	Web Security Appliance Wsa	8.0.8-mr-113	All	All	All
Application	Cisco	Web Security Appliance Wsa	8.5.0-497	All	All	All
Application	Cisco	Web Security Appliance Wsa	8.5.0.000	All	All	All
Application	Cisco	Web Security Appliance Wsa	8.5.1-021	All	All	All
Application	Cisco	Web Security Appliance Wsa	8.5.2-024	All	All	All
Application	Cisco	Web Security Appliance Wsa	8.5.2-027	All	All	All
Application	Cisco	Web Security Appliance Wsa	8.5.3-055	All	All	All
Application	Cisco	Web Security Appliance Wsa	5.6.0-623	All	All	All
Application	Cisco	Web Security Appliance Wsa	6.0.0-000	All	All	All
Application	Cisco	Web Security Appliance Wsa	7.1.0	All	All	All
Application	Cisco	Web Security Appliance Wsa	7.1.1	All	All	All
Application	Cisco	Web Security Appliance Wsa	7.1.2	All	All	All
Application	Cisco	Web Security Appliance Wsa	7.1.3	All	All	All
Application	Cisco	Web Security Appliance Wsa	7.1.4	All	All	All
Application	Cisco	Web Security Appliance Wsa	7.5.0-000	All	All	All
Application	Cisco	Web Security Appliance Wsa	7.5.0-825	All	All	All
Application	Cisco	Web Security Appliance Wsa	7.5.1-000	All	All	All
Application	Cisco	Web Security Appliance Wsa	7.5.2-000	All	All	All
Application	Cisco	Web Security Appliance Wsa	7.7.0-000	All	All	All
Application	Cisco	Web Security Appliance Wsa	7.7.1-000	All	All	All
Application	Cisco	Web Security Appliance Wsa	8.0.0-000	All	All	All
Application	Cisco	Web Security Appliance Wsa	8.0.5	All	All	All
Application	Cisco	Web Security Appliance Wsa	8.0.6	All	All	All
Application	Cisco	Web Security Appliance Wsa	8.0.6-078	All	All	All
Application	Cisco	Web Security Appliance Wsa	8.0.6-119	All	All	All
Application	Cisco	Web Security Appliance Wsa	8.0.7	All	All	All
Application	Cisco	Web Security Appliance Wsa	8.0.7-142	All	All	All
Application	Cisco	Web Security Appliance Wsa	8.0.8-mr-113	All	All	All
Application	Cisco	Web Security Appliance Wsa	8.5.0-497	All	All	All
Application	Cisco	Web Security Appliance Wsa	8.5.0.000	All	All	All

Application	Cisco	Web Security Appliance Wsa	8.5.1-021	All	All	All
Application	Cisco	Web Security Appliance Wsa	8.5.2-024	All	All	All
Application	Cisco	Web Security Appliance Wsa	8.5.2-027	All	All	All
Application	Cisco	Web Security Appliance Wsa	8.5.3-055	All	All	All
Application	Cisco	Web Security Appliance Wsa	5.6.0-623	All	All	All
Application	Cisco	Web Security Appliance Wsa	6.0.0-000	All	All	All
Application	Cisco	Web Security Appliance Wsa	7.1.0	All	All	All
Application	Cisco	Web Security Appliance Wsa	7.1.1	All	All	All
Application	Cisco	Web Security Appliance Wsa	7.1.2	All	All	All
Application	Cisco	Web Security Appliance Wsa	7.1.3	All	All	All
Application	Cisco	Web Security Appliance Wsa	7.1.4	All	All	All
Application	Cisco	Web Security Appliance Wsa	7.5.0-000	All	All	All
Application	Cisco	Web Security Appliance Wsa	7.5.0-825	All	All	All
Application	Cisco	Web Security Appliance Wsa	7.5.1-000	All	All	All
Application	Cisco	Web Security Appliance Wsa	7.5.2-000	All	All	All
Application	Cisco	Web Security Appliance Wsa	7.7.0-000	All	All	All
Application	Cisco	Web Security Appliance Wsa	7.7.1-000	All	All	All
Application	Cisco	Web Security Appliance Wsa	8.0.0-000	All	All	All
Application	Cisco	Web Security Appliance Wsa	8.0.5	All	All	All
Application	Cisco	Web Security Appliance Wsa	8.0.6	All	All	All
Application	Cisco	Web Security Appliance Wsa	8.0.6-078	All	All	All
Application	Cisco	Web Security Appliance Wsa	8.0.6-119	All	All	All
Application	Cisco	Web Security Appliance Wsa	8.0.7	All	All	All
Application	Cisco	Web Security Appliance Wsa	8.0.7-142	All	All	All
Application	Cisco	Web Security Appliance Wsa	8.0.8-mr-113	All	All	All
Application	Cisco	Web Security Appliance Wsa	8.5.0-497	All	All	All
Application	Cisco	Web Security Appliance Wsa	8.5.0.000	All	All	All
Application	Cisco	Web Security Appliance Wsa	8.5.1-021	All	All	All
Application	Cisco	Web Security Appliance Wsa	8.5.2-024	All	All	All
Application	Cisco	Web Security Appliance Wsa	8.5.2-027	All	All	All
Application	Cisco	Web Security Appliance Wsa	8.5.3-055	All	All	All

References

Reference

Cisco Web Security Appliance HTTP Response Code Processing Flaw Lets Remote Users Consume Excessive Memory Resources - Security

Cisco Web Security Appliance Connection Denial of Service Vulnerability

CVE Program record
NVD vulnerability detail
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](#)