



CVE-2015-6321

Published on: 11/05/2015 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:16 PM UTC

CVE-2015-6321

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [Content Security Management Appliance](#) from [Cisco](#) contain the following vulnerability:

Cisco AsyncOS before 8.5.7-042, 9.x before 9.1.0-032, 9.1.x before 9.1.1-023, and 9.5.x and 9.6.x before 9.6.0-042 on Email Security Appliance (ESA) devices; before 9.1.0-032, 9.1.1 before 9.1.1-005, and 9.5.x before 9.5.0-025 on Content Security Management Appliance (SMA) devices; and before 7.7.0-725 and 8.x before 8.0.8-113 on Web

Security Appliance (WSA) devices allows remote attackers to cause a denial of service (memory consumption) via a flood of TCP packets, aka Bug IDs CSCus79774, CSCus79777, and CSCzv95795.

CVE-2015-6321 has been assigned by [psirt@cisco.com](#) to track the vulnerability

CVSS2 Score: **7.8 - HIGH**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	NONE	COMPLETE

CVE References

Description	Tags	Link
Cisco Email Security Appliance TCP Flood Handling Lets Remote Users Consume Excessive Memory Resources - SecurityTracker	www.securitytracker.com text/html	SECTrack 1034060
Cisco AsyncOS TCP Flood Denial of Service Vulnerability	Vendor Advisory tools.cisco.com text/html	CISCO 20151104 Cisco AsyncOS TCP Flood Denial of Service Vulnerability
Cisco Web Security Appliance AsyncOS TCP Flood Handling Lets Remote Users Consume Excessive Memory Resources - SecurityTracker	www.securitytracker.com text/html	SECTrack 1034061

By selecting these links, you may be leaving CVEreport webpage. We have provided these links to other websites because they may have information that

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
Application	Cisco	Content Security Management Appliance	7.8.0-328	All	All	All
Application	Cisco	Content Security Management Appliance	7.8.1-001	All	All	All
Application	Cisco	Content Security Management Appliance	7.9.0-201	All	All	All
Application	Cisco	Content Security Management Appliance	7.9.2-116	All	All	All
Application	Cisco	Content Security Management Appliance	8.0.1-031	All	All	All
Application	Cisco	Content Security Management Appliance	8.1.0-001	All	All	All
Application	Cisco	Content Security Management Appliance	8.1.1-033	All	All	All
Application	Cisco	Content Security Management Appliance	8.1.2-000	All	All	All
Application	Cisco	Content Security Management Appliance	8.2.0-238	All	All	All
Application	Cisco	Content Security Management Appliance	8.3.0-350	All	All	All
Application	Cisco	Content Security Management Appliance	8.3.5-061	All	All	All
Application	Cisco	Content Security Management Appliance	8.3.6-014	All	All	All
Application	Cisco	Content Security Management Appliance	8.3.7-010	All	All	All
Application	Cisco	Content Security Management Appliance	8.4.0-150	All	All	All
Application	Cisco	Content Security Management Appliance	9.0.0-073	All	All	All
Application	Cisco	Content Security Management Appliance	9.1.0-004	All	All	All
Application	Cisco	Content Security Management Appliance	7.8.0-328	All	All	All
Application	Cisco	Content Security Management Appliance	7.8.1-001	All	All	All
Application	Cisco	Content Security Management Appliance	7.9.0-201	All	All	All
Application	Cisco	Content Security Management Appliance	7.9.2-116	All	All	All
Application	Cisco	Content Security Management Appliance	8.0.1-031	All	All	All
Application	Cisco	Content Security Management Appliance	8.1.0-001	All	All	All
Application	Cisco	Content Security Management Appliance	8.1.1-033	All	All	All
Application	Cisco	Content Security Management Appliance	8.1.2-000	All	All	All
Application	Cisco	Content Security Management Appliance	8.2.0-238	All	All	All
Application	Cisco	Content Security Management Appliance	8.3.0-350	All	All	All
Application	Cisco	Content Security Management Appliance	8.3.5-061	All	All	All
Application	Cisco	Content Security Management Appliance	8.3.6-014	All	All	All

Application	Cisco	Content Security Management Appliance	8.3.7-010	All	All	All
Application	Cisco	Content Security Management Appliance	8.4.0-150	All	All	All
Application	Cisco	Content Security Management Appliance	9.0.0-073	All	All	All
Application	Cisco	Content Security Management Appliance	9.1.0-004	All	All	All
Application	Cisco	Email Security Appliance	7.6.1-000	All	All	All
Application	Cisco	Email Security Appliance	7.6.3-000	All	All	All
Application	Cisco	Email Security Appliance	7.7.0-000	All	All	All
Application	Cisco	Email Security Appliance	7.7.1-000	All	All	All
Application	Cisco	Email Security Appliance	7.8.0-311	All	All	All
Application	Cisco	Email Security Appliance	8.5.6-052	All	All	All
Application	Cisco	Email Security Appliance	8.6.0-011	All	All	All
Application	Cisco	Email Security Appliance	8.9.1-000	All	All	All
Application	Cisco	Email Security Appliance	8.9.2-032	All	All	All
Application	Cisco	Email Security Appliance	9.0.0-212	All	All	All
Application	Cisco	Email Security Appliance	9.0.5-000	All	All	All
Application	Cisco	Email Security Appliance	9.1.0-011	All	All	All
Application	Cisco	Email Security Appliance	9.4.4-000	All	All	All
Application	Cisco	Email Security Appliance	9.5.0-000	All	All	All
Application	Cisco	Email Security Appliance	7.6.1-000	All	All	All
Application	Cisco	Email Security Appliance	7.6.3-000	All	All	All
Application	Cisco	Email Security Appliance	7.7.0-000	All	All	All
Application	Cisco	Email Security Appliance	7.7.1-000	All	All	All
Application	Cisco	Email Security Appliance	7.8.0-311	All	All	All
Application	Cisco	Email Security Appliance	8.5.6-052	All	All	All
Application	Cisco	Email Security Appliance	8.6.0-011	All	All	All
Application	Cisco	Email Security Appliance	8.9.1-000	All	All	All
Application	Cisco	Email Security Appliance	8.9.2-032	All	All	All
Application	Cisco	Email Security Appliance	9.0.0-212	All	All	All
Application	Cisco	Email Security Appliance	9.0.5-000	All	All	All
Application	Cisco	Email Security Appliance	9.1.0-011	All	All	All
Application	Cisco	Email Security Appliance	9.4.4-000	All	All	All
Application	Cisco	Email Security Appliance	9.5.0-000	All	All	All
Application	Cisco	Web Security Appliance	5.6.0-623	All	All	All
Application	Cisco	Web Security Appliance	6.0.0-000	All	All	All
Application	Cisco	Web Security Appliance	7.5.0-000	All	All	All
Application	Cisco	Web Security Appliance	7.5.0-005	All	All	All

Application	Cisco	Web Security Appliance	7.5.0-825	All	All	All
Application	Cisco	Web Security Appliance	7.5.1-000	All	All	All
Application	Cisco	Web Security Appliance	7.5.2-000	All	All	All
Application	Cisco	Web Security Appliance	7.7.0-000	All	All	All
Application	Cisco	Web Security Appliance	7.7.1-000	All	All	All
Application	Cisco	Web Security Appliance	8.0.0-000	All	All	All
Application	Cisco	Web Security Appliance	8.5.0.000	All	All	All
Application	Cisco	Web Security Appliance	5.6.0-623	All	All	All
Application	Cisco	Web Security Appliance	6.0.0-000	All	All	All
Application	Cisco	Web Security Appliance	7.5.0-000	All	All	All
Application	Cisco	Web Security Appliance	7.5.0-825	All	All	All
Application	Cisco	Web Security Appliance	7.5.1-000	All	All	All
Application	Cisco	Web Security Appliance	7.5.2-000	All	All	All
Application	Cisco	Web Security Appliance	7.7.0-000	All	All	All
Application	Cisco	Web Security Appliance	7.7.1-000	All	All	All
Application	Cisco	Web Security Appliance	8.0.0-000	All	All	All
Application	Cisco	Web Security Appliance	8.5.0.000	All	All	All
cpe:2.3:a:cisco:content_security_management_appliance:7.8.0-328:*:*:*:*:*:						
cpe:2.3:a:cisco:content_security_management_appliance:7.8.1-001:*:*:*:*:*:						
cpe:2.3:a:cisco:content_security_management_appliance:7.9.0-201:*:*:*:*:*:						
cpe:2.3:a:cisco:content_security_management_appliance:7.9.2-116:*:*:*:*:*:						
cpe:2.3:a:cisco:content_security_management_appliance:8.0.1-031:*:*:*:*:*:						
cpe:2.3:a:cisco:content_security_management_appliance:8.1.0-001:*:*:*:*:*:						
cpe:2.3:a:cisco:content_security_management_appliance:8.1.1-033:*:*:*:*:*:						
cpe:2.3:a:cisco:content_security_management_appliance:8.1.2-000:*:*:*:*:*:						
cpe:2.3:a:cisco:content_security_management_appliance:8.2.0-238:*:*:*:*:*:						
cpe:2.3:a:cisco:content_security_management_appliance:8.3.0-350:*:*:*:*:*:						
cpe:2.3:a:cisco:content_security_management_appliance:8.3.5-061:*:*:*:*:*:						
cpe:2.3:a:cisco:content_security_management_appliance:8.3.6-014:*:*:*:*:*:						
cpe:2.3:a:cisco:content_security_management_appliance:8.3.7-010:*:*:*:*:*:						
cpe:2.3:a:cisco:content_security_management_appliance:8.4.0-150:*:*:*:*:*:						
cpe:2.3:a:cisco:content_security_management_appliance:9.0.0-073:*:*:*:*:*:						

cpe:2.3:a:cisco:content_security_management_appliance:9.1.0-004:*****:
cpe:2.3:a:cisco:content_security_management_appliance:7.8.0-328:*****:
cpe:2.3:a:cisco:content_security_management_appliance:7.8.1-001:*****:
cpe:2.3:a:cisco:content_security_management_appliance:7.9.0-201:*****:
cpe:2.3:a:cisco:content_security_management_appliance:7.9.2-116:*****:
cpe:2.3:a:cisco:content_security_management_appliance:8.0.1-031:*****:
cpe:2.3:a:cisco:content_security_management_appliance:8.1.0-001:*****:
cpe:2.3:a:cisco:content_security_management_appliance:8.1.1-033:*****:
cpe:2.3:a:cisco:content_security_management_appliance:8.1.2-000:*****:
cpe:2.3:a:cisco:content_security_management_appliance:8.2.0-238:*****:
cpe:2.3:a:cisco:content_security_management_appliance:8.3.0-350:*****:
cpe:2.3:a:cisco:content_security_management_appliance:8.3.5-061:*****:
cpe:2.3:a:cisco:content_security_management_appliance:8.3.6-014:*****:
cpe:2.3:a:cisco:content_security_management_appliance:8.3.7-010:*****:
cpe:2.3:a:cisco:content_security_management_appliance:8.4.0-150:*****:
cpe:2.3:a:cisco:content_security_management_appliance:9.0.0-073:*****:
cpe:2.3:a:cisco:content_security_management_appliance:9.1.0-004:*****:
cpe:2.3:a:cisco:email_security_appliance:7.6.1-000:*****:
cpe:2.3:a:cisco:email_security_appliance:7.6.3-000:*****:
cpe:2.3:a:cisco:email_security_appliance:7.7.0-000:*****:
cpe:2.3:a:cisco:email_security_appliance:7.7.1-000:*****:
cpe:2.3:a:cisco:email_security_appliance:7.8.0-311:*****:
cpe:2.3:a:cisco:email_security_appliance:8.5.6-052:*****:
cpe:2.3:a:cisco:email_security_appliance:8.6.0-011:*****:
cpe:2.3:a:cisco:email_security_appliance:8.9.1-000:*****:
cpe:2.3:a:cisco:email_security_appliance:8.9.2-032:*****:
cpe:2.3:a:cisco:email_security_appliance:9.0.0-212:*****:
cpe:2.3:a:cisco:email_security_appliance:9.0.5-000:*****:
cpe:2.3:a:cisco:email_security_appliance:9.1.0-011:*****:

cpe:2.3:a:cisco:email_security_appliance:9.1.0-011:*****:
cpe:2.3:a:cisco:email_security_appliance:9.4.4-000:*****:
cpe:2.3:a:cisco:email_security_appliance:9.5.0-000:*****:
cpe:2.3:a:cisco:email_security_appliance:7.6.1-000:*****:
cpe:2.3:a:cisco:email_security_appliance:7.6.3-000:*****:
cpe:2.3:a:cisco:email_security_appliance:7.7.0-000:*****:
cpe:2.3:a:cisco:email_security_appliance:7.7.1-000:*****:
cpe:2.3:a:cisco:email_security_appliance:7.8.0-311:*****:
cpe:2.3:a:cisco:email_security_appliance:8.5.6-052:*****:
cpe:2.3:a:cisco:email_security_appliance:8.6.0-011:*****:
cpe:2.3:a:cisco:email_security_appliance:8.9.1-000:*****:
cpe:2.3:a:cisco:email_security_appliance:8.9.2-032:*****:
cpe:2.3:a:cisco:email_security_appliance:9.0.0-212:*****:
cpe:2.3:a:cisco:email_security_appliance:9.0.5-000:*****:
cpe:2.3:a:cisco:email_security_appliance:9.1.0-011:*****:
cpe:2.3:a:cisco:email_security_appliance:9.4.4-000:*****:
cpe:2.3:a:cisco:email_security_appliance:9.5.0-000:*****:
cpe:2.3:a:cisco:web_security_appliance:5.6.0-623:*****:
cpe:2.3:a:cisco:web_security_appliance:6.0.0-000:*****:
cpe:2.3:a:cisco:web_security_appliance:7.5.0-000:*****:
cpe:2.3:a:cisco:web_security_appliance:7.5.0-825:*****:
cpe:2.3:a:cisco:web_security_appliance:7.5.1-000:*****:
cpe:2.3:a:cisco:web_security_appliance:7.5.2-000:*****:
cpe:2.3:a:cisco:web_security_appliance:7.7.0-000:*****:
cpe:2.3:a:cisco:web_security_appliance:7.7.1-000:*****:
cpe:2.3:a:cisco:web_security_appliance:8.0.0-000:*****:
cpe:2.3:a:cisco:web_security_appliance:8.5.0.000:*****:
cpe:2.3:a:cisco:web_security_appliance:5.6.0-623:*****:
cpe:2.3:a:cisco:web_security_appliance:6.0.0-000:*****:

cpe:2.3:a:cisco:web_security_appliance:7.5.0-000:*****:
cpe:2.3:a:cisco:web_security_appliance:7.5.0-825:*****:
cpe:2.3:a:cisco:web_security_appliance:7.5.1-000:*****:
cpe:2.3:a:cisco:web_security_appliance:7.5.2-000:*****:
cpe:2.3:a:cisco:web_security_appliance:7.7.0-000:*****:
cpe:2.3:a:cisco:web_security_appliance:7.7.1-000:*****:
cpe:2.3:a:cisco:web_security_appliance:8.0.0-000:*****:
cpe:2.3:a:cisco:web_security_appliance:8.5.0.000:*****:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID→](#)