



CVE-2017-12219

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

Summary

CVE	CVE-2017-12219
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-09-21 05:29:00 UTC
Updated	2019-10-09 23:22:00 UTC
Description	A vulnerability in the handling of IP fragments for the Cisco Small Business SPA300, SPA500, and SPA51x Series IP Phon

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Cisco	Spa 301	-	All	All	All
Hardware	Cisco	Spa 301	-	All	All	All
Operating System	Cisco	Spa 301 Firmware	7.6.2	All	All	All
Operating System	Cisco	Spa 301 Firmware	7.6.2	All	All	All
Hardware	Cisco	Spa 303	-	All	All	All
Hardware	Cisco	Spa 303	-	All	All	All
Operating System	Cisco	Spa 303 Firmware	7.6.2	All	All	All
Operating System	Cisco	Spa 303 Firmware	7.6.2	All	All	All
Hardware	Cisco	Spa 500ds	-	All	All	All
Hardware	Cisco	Spa 500ds	-	All	All	All
Operating System	Cisco	Spa 500ds Firmware	7.6.2	All	All	All
Operating System	Cisco	Spa 500ds Firmware	7.6.2	All	All	All
Hardware	Cisco	Spa 500s	-	All	All	All
Hardware	Cisco	Spa 500s	-	All	All	All
Operating System	Cisco	Spa 500s Firmware	7.6.2	All	All	All
Operating System	Cisco	Spa 500s Firmware	7.6.2	All	All	All
Hardware	Cisco	Spa 501g	-	All	All	All

Hardware	Cisco	Spa 501g	-	All	All	All
Operating System	Cisco	Spa 501g Firmware	7.6.2	All	All	All
Operating System	Cisco	Spa 501g Firmware	7.6.2	All	All	All
Hardware	Cisco	Spa 502g	-	All	All	All
Hardware	Cisco	Spa 502g	-	All	All	All
Operating System	Cisco	Spa 502g Firmware	7.6.2	All	All	All
Operating System	Cisco	Spa 502g Firmware	7.6.2	All	All	All
Hardware	Cisco	Spa 504g	-	All	All	All
Hardware	Cisco	Spa 504g	-	All	All	All
Operating System	Cisco	Spa 504g Firmware	7.6.2	All	All	All
Operating System	Cisco	Spa 504g Firmware	7.6.2	All	All	All
Hardware	Cisco	Spa 508g	-	All	All	All
Hardware	Cisco	Spa 508g	-	All	All	All
Operating System	Cisco	Spa 508g Firmware	7.6.2	All	All	All
Operating System	Cisco	Spa 508g Firmware	7.6.2	All	All	All
Hardware	Cisco	Spa 509g	-	All	All	All
Hardware	Cisco	Spa 509g	-	All	All	All
Operating System	Cisco	Spa 509g Firmware	7.6.2	All	All	All
Operating System	Cisco	Spa 509g Firmware	7.6.2	All	All	All
Hardware	Cisco	Spa 512g	-	All	All	All
Hardware	Cisco	Spa 512g	-	All	All	All
Operating System	Cisco	Spa 512g Firmware	7.6.2	All	All	All
Operating System	Cisco	Spa 512g Firmware	7.6.2	All	All	All
Hardware	Cisco	Spa 514g	-	All	All	All
Hardware	Cisco	Spa 514g	-	All	All	All
Operating System	Cisco	Spa 514g Firmware	7.6.2	All	All	All
Operating System	Cisco	Spa 514g Firmware	7.6.2	All	All	All

References

Reference

Multiple Cisco Products CVE-2017-12219 Denial of Service Vulnerability

Cisco Small Business SPA300, SPA500, and SPA51x Series IP Phones Denial of Service Vulnerability

Cisco Small Business SPA300, SPA500, and SPA51x Series IP Phones Lets Remote Users Cause the Target System to Reload - SecurityTrails
 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](#)