



# CVE-2018-0209

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

## Summary

<b>CVE</b>	CVE-2018-0209
<b>State</b>	PUBLIC
<b>Assigner</b>	psirt@cisco.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2018-03-08 07:29:00 UTC
<b>Updated</b>	2020-10-22 16:13:00 UTC
<b>Description</b>	A vulnerability in the Simple Network Management Protocol (SNMP) subsystem communication channel through the Cisco

## Risk And Classification

**Problem Types:** NVD-CWE-Other

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Cisco	Sf500-24	-	All	All	All
Hardware	Cisco	Sf500-24	-	All	All	All
Hardware	Cisco	Sf500-24mp	-	All	All	All
Hardware	Cisco	Sf500-24mp	-	All	All	All
Hardware	Cisco	Sf500-24p	-	All	All	All
Hardware	Cisco	Sf500-24p	-	All	All	All
Hardware	Cisco	Sf500-48	-	All	All	All
Hardware	Cisco	Sf500-48	-	All	All	All
Hardware	Cisco	Sf500-48mp	-	All	All	All
Hardware	Cisco	Sf500-48mp	-	All	All	All
Hardware	Cisco	Sf500-48p	-	All	All	All
Hardware	Cisco	Sf500-48p	-	All	All	All
Hardware	Cisco	Sg500-28	-	All	All	All
Hardware	Cisco	Sg500-28	-	All	All	All
Hardware	Cisco	Sg500-28mpp	-	All	All	All
Hardware	Cisco	Sg500-28mpp	-	All	All	All
Hardware	Cisco	Sg500-28p	-	All	All	All

Hardware	Cisco	Sg500-28p	-	All	All	All
Hardware	Cisco	Sg500-52	-	All	All	All
Hardware	Cisco	Sg500-52	-	All	All	All
Hardware	Cisco	Sg500-52mp	-	All	All	All
Hardware	Cisco	Sg500-52mp	-	All	All	All
Hardware	Cisco	Sg500-52p	-	All	All	All
Hardware	Cisco	Sg500-52p	-	All	All	All
Hardware	Cisco	Sg500x-24	-	All	All	All
Hardware	Cisco	Sg500x-24	-	All	All	All
Hardware	Cisco	Sg500x-24mpp	-	All	All	All
Hardware	Cisco	Sg500x-24mpp	-	All	All	All
Hardware	Cisco	Sg500x-24p	-	All	All	All
Hardware	Cisco	Sg500x-24p	-	All	All	All
Hardware	Cisco	Sg500x-48	-	All	All	All
Hardware	Cisco	Sg500x-48	-	All	All	All
Hardware	Cisco	Sg500x-48mp	-	All	All	All
Hardware	Cisco	Sg500x-48mp	-	All	All	All
Hardware	Cisco	Sg500x-48p	-	All	All	All
Hardware	Cisco	Sg500x-48p	-	All	All	All
Hardware	Cisco	Sg500xg-8f8t	-	All	All	All
Hardware	Cisco	Sg500xg-8f8t	-	All	All	All
Operating System	Cisco	Small Business 500 Series Stackable Managed Switches Firmware	2.2.5.68	All	All	All
Operating System	Cisco	Small Business 500 Series Stackable Managed Switches Firmware	2.3.0.130	All	All	All
Operating System	Cisco	Small Business 500 Series Stackable Managed Switches Firmware	2.2.5.68	All	All	All
Operating System	Cisco	Small Business 500 Series Stackable Managed Switches Firmware	2.3.0.130	All	All	All

## References

Reference	Source	Link	Tags
Cisco 550X Series Stackable Managed Switches CVE-2018-0209 Denial of Service Vulnerability	BID	<a href="http://www.securityfocus.com">www.securityfocus.com</a>	This
Cisco 550X Series Stackable Managed Switches SNMP Denial of Service Vulnerability	CONFIRM	<a href="http://tools.cisco.com">tools.cisco.com</a>	Ver
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>	car
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>	car

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](#)