



CVE-2019-1913

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

Summary

CVE	CVE-2019-1913
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-08-07 06:15:00 UTC
Updated	2019-10-01 23:15:00 UTC
Description	Multiple vulnerabilities in the web management interface of Cisco Small Business 220 Series Smart Switches could allow an

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Cisco	Sf-220-24	-	All	All	All
Hardware	Cisco	Sf-220-24	-	All	All	All
Operating System	Cisco	Sf-220-24 Firmware	All	All	All	All
Operating System	Cisco	Sf-220-24 Firmware	All	All	All	All
Hardware	Cisco	Sf220-24p	-	All	All	All
Hardware	Cisco	Sf220-24p	-	All	All	All
Operating System	Cisco	Sf220-24p Firmware	All	All	All	All
Operating System	Cisco	Sf220-24p Firmware	All	All	All	All
Hardware	Cisco	Sf220-48	-	All	All	All
Hardware	Cisco	Sf220-48	-	All	All	All
Hardware	Cisco	Sf220-48p	-	All	All	All
Hardware	Cisco	Sf220-48p	-	All	All	All
Operating System	Cisco	Sf220-48p Firmware	All	All	All	All
Operating System	Cisco	Sf220-48p Firmware	All	All	All	All
Operating System	Cisco	Sf220-48 Firmware	All	All	All	All
Operating System	Cisco	Sf220-48 Firmware	All	All	All	All
Hardware	Cisco	Sg220-26	-	All	All	All

Hardware	Cisco	Sg220-26	-	All	All	All
Hardware	Cisco	Sg220-26p	-	All	All	All
Hardware	Cisco	Sg220-26p	-	All	All	All
Operating System	Cisco	Sg220-26p Firmware	All	All	All	All
Operating System	Cisco	Sg220-26p Firmware	All	All	All	All
Operating System	Cisco	Sg220-26 Firmware	All	All	All	All
Operating System	Cisco	Sg220-26 Firmware	All	All	All	All
Hardware	Cisco	Sg220-28	-	All	All	All
Hardware	Cisco	Sg220-28	-	All	All	All
Hardware	Cisco	Sg220-28mp	-	All	All	All
Hardware	Cisco	Sg220-28mp	-	All	All	All
Operating System	Cisco	Sg220-28mp Firmware	All	All	All	All
Operating System	Cisco	Sg220-28mp Firmware	All	All	All	All
Operating System	Cisco	Sg220-28 Firmware	All	All	All	All
Operating System	Cisco	Sg220-28 Firmware	All	All	All	All
Hardware	Cisco	Sg220-50	-	All	All	All
Hardware	Cisco	Sg220-50	-	All	All	All
Hardware	Cisco	Sg220-50p	-	All	All	All
Hardware	Cisco	Sg220-50p	-	All	All	All
Operating System	Cisco	Sg220-50p Firmware	All	All	All	All
Operating System	Cisco	Sg220-50p Firmware	All	All	All	All
Operating System	Cisco	Sg220-50 Firmware	All	All	All	All
Operating System	Cisco	Sg220-50 Firmware	All	All	All	All
Hardware	Cisco	Sg220-52	-	All	All	All
Hardware	Cisco	Sg220-52	-	All	All	All
Operating System	Cisco	Sg220-52 Firmware	All	All	All	All
Operating System	Cisco	Sg220-52 Firmware	All	All	All	All

References						
Reference			Source	Link	Tags	
Cisco Small Business 220 Series Smart Switches Remote Code Execution Vulnerabilities			CISCO	tools.cisco.com	Vendor A	
Realtek Managed Switch Controller (RTL83xx) Stack Overflow ~ Packet Storm			MISC	packetstormsecurity.com		
CVE Program record			CVE.ORG	www.cve.org	canonica	
NVD vulnerability detail			NVD	nvd.nist.gov	canonica	

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](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)