



CVE-2021-34757

Published on: 10/06/2021 12:00:00 AM UTC

Last Modified on: 10/24/2022 02:26:00 PM UTC

CVE-2021-34757 - advisory for cisco-sa-sb-hardcoded-cred-MJCEXvX

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

CVSS:31/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N



Certain versions of [Business 220-16p-2g](#) from [Cisco](#) contain the following vulnerability:

Multiple vulnerabilities in Cisco Business 220 Series Smart Switches firmware could allow an attacker with Administrator privileges to access sensitive login credentials or reconfigure the passwords on the user account. For more information about these vulnerabilities, see the Details section of this advisory.

CVE-2021-34757 has been assigned by [Cisco PSIRT](#) to track the vulnerability - currently rated as **MEDIUM** severity.

The Cisco PSIRT is not aware of any public announcements or malicious use of the vulnerabilities that are described in this advisory.

Affected Vendor/Software: [Cisco](#) - **Cisco Small Business 220 Series Smart Plus Switches** version **n/a**

CVSS3 Score: **5.5 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
PHYSICAL	LOW	HIGH	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	NONE

CVSS2 Score: **3.6 - LOW**

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	NONE

CVE References

Description	Tags	Link
-------------	------	------

Cisco Business 220 Series Smart Switches Static Key and Password Vulnerabilities

[tools.cisco.com](#)
[text/html](#)

 [CISCO 20211006 Cisco Business 220 Series Smart Switches Static Key and Password Vulnerabilities](#)

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.

Related QID Numbers

730230 Cisco Business 220 Series Smart Switches Static Key and Password Vulnerabilities (cisco-sa-sb-hardcoded-cred-MJCEXvX)

Exploit/POC from Github

Multiple vulnerabilities in Cisco Business 220 Series Smart Switches firmware could allow an attacker with Administra...

Known Affected Configurations (CPE V2.3)						
Type	Vendor	Product	Version	Update	Edition	Language
Hardware 	Cisco	Business 220-16p-2g	-	All	All	All
Operating System	Cisco	Business 220-16p-2g Firmware	All	All	All	All
Hardware 	Cisco	Business 220-16t-2g	-	All	All	All
Operating System	Cisco	Business 220-16t-2g Firmware	All	All	All	All
Hardware 	Cisco	Business 220-24fp-4g	-	All	All	All
Operating System	Cisco	Business 220-24fp-4g Firmware	All	All	All	All
Hardware 	Cisco	Business 220-24fp-4x	-	All	All	All
Operating System	Cisco	Business 220-24fp-4x Firmware	All	All	All	All
Hardware 	Cisco	Business 220-24p-4g	-	All	All	All
Operating System	Cisco	Business 220-24p-4g Firmware	All	All	All	All
Hardware 	Cisco	Business 220-24p-4x	-	All	All	All
Operating System	Cisco	Business 220-24p-4x Firmware	All	All	All	All
Hardware 	Cisco	Business 220-24t-4g	-	All	All	All
Operating System	Cisco	Business 220-24t-4g Firmware	All	All	All	All
Hardware 	Cisco	Business 220-24t-4x	-	All	All	All
Operating	Cisco	Business 220-24t-4x Firmware	All	All	All	All

System						
Hardware 	Cisco	Business 220-48fp-4x	-	All	All	All
Operating System	Cisco	Business 220-48fp-4x Firmware	All	All	All	All
Hardware 	Cisco	Business 220-48p-4g	-	All	All	All
Operating System	Cisco	Business 220-48p-4g Firmware	All	All	All	All
Hardware 	Cisco	Business 220-48p-4x	-	All	All	All
Operating System	Cisco	Business 220-48p-4x Firmware	All	All	All	All
Hardware 	Cisco	Business 220-48t-4g	-	All	All	All
Operating System	Cisco	Business 220-48t-4g Firmware	All	All	All	All
Hardware 	Cisco	Business 220-48t-4x	-	All	All	All
Operating System	Cisco	Business 220-48t-4x Firmware	All	All	All	All
Hardware 	Cisco	Business 220-8fp-e-2g	-	All	All	All
Operating System	Cisco	Business 220-8fp-e-2g Firmware	All	All	All	All
Hardware 	Cisco	Business 220-8p-e-2g	-	All	All	All
Operating System	Cisco	Business 220-8p-e-2g Firmware	All	All	All	All
Hardware 	Cisco	Business 220-8t-e-2g	-	All	All	All
Operating System	Cisco	Business 220-8t-e-2g Firmware	All	All	All	All
cpe:2.3:h:cisco:business_220-16p-2g:-:*:*:*:*:*:						
cpe:2.3:o:cisco:business_220-16p-2g_firmware:*:*:*:*:*:						
cpe:2.3:h:cisco:business_220-16t-2g:-:*:*:*:*:*:						
cpe:2.3:o:cisco:business_220-16t-2g_firmware:*:*:*:*:*:						
cpe:2.3:h:cisco:business_220-24fp-4g:-:*:*:*:*:*:						
cpe:2.3:o:cisco:business_220-24fp-4g_firmware:*:*:*:*:*:						
cpe:2.3:h:cisco:business_220-24fp-4x:-:*:*:*:*:*:						
cpe:2.3:o:cisco:business_220-24fp-4x_firmware:*:*:*:*:*:						
cpe:2.3:h:cisco:business_220-24p-4g:-:*:*:*:*:*:						
cpe:2.3:o:cisco:business_220-24p-4g_firmware:*:*:*:*:*:						
cpe:2.3:h:cisco:business_220-24p-4x:-:*:*:*:*:*:						

cpe:2.3:o:cisco:business_220-24p-4x_firmware:*.*.*.*.*.*.*.*.
cpe:2.3:h:cisco:business_220-24t-4g:-.*.*.*.*.*.*.*.*.
cpe:2.3:o:cisco:business_220-24t-4g_firmware:*.*.*.*.*.*.*.*.
cpe:2.3:h:cisco:business_220-24t-4x:-.*.*.*.*.*.*.*.*.
cpe:2.3:o:cisco:business_220-24t-4x_firmware:*.*.*.*.*.*.*.*.
cpe:2.3:h:cisco:business_220-48fp-4x:-.*.*.*.*.*.*.*.*.
cpe:2.3:o:cisco:business_220-48fp-4x_firmware:*.*.*.*.*.*.*.*.
cpe:2.3:h:cisco:business_220-48p-4g:-.*.*.*.*.*.*.*.*.
cpe:2.3:o:cisco:business_220-48p-4g_firmware:*.*.*.*.*.*.*.*.
cpe:2.3:h:cisco:business_220-48p-4x:-.*.*.*.*.*.*.*.*.
cpe:2.3:o:cisco:business_220-48p-4x_firmware:*.*.*.*.*.*.*.*.
cpe:2.3:h:cisco:business_220-48t-4g:-.*.*.*.*.*.*.*.*.
cpe:2.3:o:cisco:business_220-48t-4g_firmware:*.*.*.*.*.*.*.*.
cpe:2.3:h:cisco:business_220-48t-4x:-.*.*.*.*.*.*.*.*.
cpe:2.3:o:cisco:business_220-48t-4x_firmware:*.*.*.*.*.*.*.*.
cpe:2.3:h:cisco:business_220-8fp-e-2g:-.*.*.*.*.*.*.*.*.
cpe:2.3:o:cisco:business_220-8fp-e-2g_firmware:*.*.*.*.*.*.*.*.
cpe:2.3:h:cisco:business_220-8p-e-2g:-.*.*.*.*.*.*.*.*.
cpe:2.3:o:cisco:business_220-8p-e-2g_firmware:*.*.*.*.*.*.*.*.
cpe:2.3:h:cisco:business_220-8t-e-2g:-.*.*.*.*.*.*.*.*.
cpe:2.3:o:cisco:business_220-8t-e-2g_firmware:*.*.*.*.*.*.*.*.

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
🔍 @CVEreport	CVE-2021-34757 : Multiple vulnerabilities in Cisco Business 220 Series Smart Switches firmware could allow an attac... twitter.com/i/web/status/1...	2021-10-06 20:02:52

[← Previous ID](#)

Next ID→

© [CVE.report](#) 2023   |

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](#)