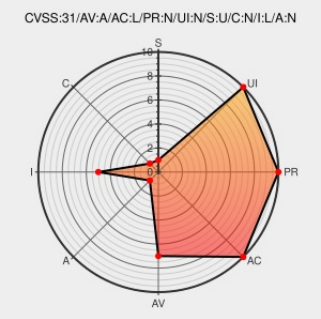
CVE-2021-34779

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

Last Modified on: 10/14/2021 07:58:00 PM UTC

CVE-2021-34779 - advisory for cisco-sa-sb220-lldp-multivuls-mVRUtQ8T

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Business 220-16p-2g from Cisco contain the following vulnerability:

Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities.

CVE-2021-34779 has been assigned by psirt@cisco.com to track the vulnerability - currently rated as HIGH 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 200 Series Smart Switches** version **n/a**

CVSS3 Score: 8.8 - HIGH

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

CVSS2 Score: 7.9 - HIGH

Access Vector	Access Complexity	Authentication
ADJACENT_NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**

COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
Cisco Small Business 220 Series Smart Switches Link Layer Discovery Protocol Vulnerabilities	tools.cisco.com text/html	CISCO 20211006 Cisco Small Business 220 Series Smart Switches Link Layer Discovery Protocol Vulnerabilities

Related QID Numbers

730223 Cisco Small Business 220 Series Smart Switches Link Layer Discovery Protocol Vulnerabilities (cisco-sa-sb220-lldp-multivuls-mVRUtQ8T)

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 System	Cisco	Business 220-24t-4x Firmware	All	All	All	All

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-2021-34779 : Multiple vulnerabilities exist in the Link Layer Discovery Protocol LLDP implementation for Cisc… twitter.com/i/web/status/1…	2021-10-06 19:56:01
@ohhara_shiojiri	"Two high-severity issues (CVE-2021-34779, CVE-2021-34780) were found in the Link Layer Discovery Protocol (LLDP) i… twitter.com/i/web/status/1…	2021-10-08 05:17:18

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report