



CVE-2019-5024

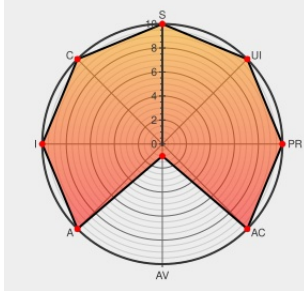
Published on: 04/11/2019 12:00:00 AM UTC

Last Modified on: 06/13/2022 06:46:00 PM UTC

CVE-2019-5024

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

CVSS:30/AV:P/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H



Certain versions of [Smartlinx Neuron 2](#) from [Capsuletech](#) contain the following vulnerability:

A restricted environment escape vulnerability exists in the “kiosk mode” function of Capsule Technologies SmartLinx Neuron 2 medical information collection devices running versions 9.0.3 or lower. A specific series of keyboard inputs can escape the restricted environment, resulting in full administrator access to the underlying

operating system. An attacker can connect to the device via USB port with a keyboard or other HID device to trigger this vulnerability.

CVE-2019-5024 has been assigned by [cisco](#) talos-cna@cisco.com to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: [cisco](#) **Capsule Technologies - Capsule Technologies SmartLinx Neuron 2 version 9.0.3 or lower**

CVSS3 Score: **7.6 - HIGH**

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

CVSS2 Score: **7.2 - HIGH**

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

CVE References

Description

TALOS-2019-0785 || Cisco Talos Intelligence Group - Comprehensive Threat Intelligence

Tags

Third Party Advisory

talosintelligence.com

text/html

Link

CONFIRM

talosintelligence.com/vulnerability_reports/TALOS-2019-0785

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.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Capsuletech	Smartlinx Neuron 2	-	All	All	All
Hardware	Capsuletech	Smartlinx Neuron 2	-	All	All	All
Operating System	Capsuletech	Smartlinx Neuron 2 Firmware	6.9.1	All	All	All
Operating System	Capsuletech	Smartlinx Neuron 2 Firmware	6.9.1	All	All	All
Operating System	Capsuletech	Smartlinx Neuron 2 Firmware	All	All	All	All
cpe:2.3:h:capsuletech:smartlinx_neuron_2:-:~::~~::~~::~~::~~::~~::~~:::						
cpe:2.3:h:capsuletech:smartlinx_neuron_2:-:~::~~::~~::~~::~~::~~::~~:::						
cpe:2.3:o:capsuletech:smartlinx_neuron_2_firmware:6.9.1:~::~~::~~::~~::~~::~~::~~:::						
cpe:2.3:o:capsuletech:smartlinx_neuron_2_firmware:6.9.1:~::~~::~~::~~::~~::~~::~~:::						
cpe:2.3:o:capsuletech:smartlinx_neuron_2_firmware:~::~~::~~::~~::~~::~~::~~:::						

No vendor comments have been submitted for this CVE

← 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](#)