



CVE-2021-25664

Published on: 04/22/2021 12:00:00 AM UTC

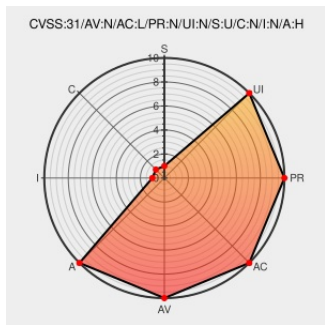
Last Modified on: 11/17/2021 10:17:00 PM UTC

CVE-2021-25664

Source: Mitre

Source: Nist

Print: PDF



Certain versions of [Capital Vstar](#) from [Siemens](#) contain the following vulnerability:

A vulnerability has been identified in Capital VSTAR (Versions including affected IPv6 stack), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus ReadyStart V4 (All versions < V4.1.0), Nucleus Source Code (Versions including affected IPv6 stack). The function that processes the Hop-by-Hop extension header in IPv6 packets and its options lacks any checks against the length field of the header, allowing attackers to put the function into an infinite loop by supplying arbitrary length values.

CVE-2021-25664 has been assigned by [S](#) productcert@siemens.com to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: [S](#) Siemens - Capital VSTAR version Versions including affected IPv6 stack

Affected Vendor/Software: [S](#) Siemens - Nucleus NET version All versions

Affected Vendor/Software: [S](#) Siemens - Nucleus ReadyStart V3 version All versions < V2017.02.4

Affected Vendor/Software: [S](#) Siemens - Nucleus ReadyStart V4 version All versions < V4.1.0

Affected Vendor/Software: [S](#) Siemens - Nucleus Source Code version Versions including affected IPv6 stack

Affected Vendor/Software: [S](#) Siemens - Nucleus Source Code version Versions including affected IPv6 stack

CVSS3 Score: **7.5 - HIGH**



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

CVSS2 Score: **5 - MEDIUM**

Access Vector	Access Complexity	Authentication

NETWORK	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	NONE	PARTIAL

CVE References

Description	Tags	Link
Siemens Nucleus Products IPv6 Stack CISA	us-cert.cisa.gov text/html	 MISC us-cert.cisa.gov/ics/advisories/icsa-21-103-05
	cert-portal.siemens.com application/pdf	 MISC cert-portal.siemens.com/productcert/pdf/ssa-248289.pdf

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
Application	Siemens	Capital Vstar	-	All	All	All
Application	Siemens	Nucleus 4	All	All	All	All
Application	Siemens	Nucleus Net	All	All	All	All
Application	Siemens	Nucleus Readystart	All	All	All	All
Application	Siemens	Nucleus Source Code	-	All	All	All
Application	Siemens	Vstar	-	All	All	All

<code>cpe:2.3:a:siemens:capital_vstar:-:*:*:*:*:*:</code>
<code>cpe:2.3:a:siemens:nucleus_4:*:*:*:*:*:</code>
<code>cpe:2.3:a:siemens:nucleus_net:*:*:*:*:*:</code>
<code>cpe:2.3:a:siemens:nucleus_readystart:*:*:*:*:*:</code>
<code>cpe:2.3:a:siemens:nucleus_source_code:-:*:*:*:*:*:</code>
<code>cpe:2.3:a:siemens:vstar:-:*:*:*:*:*:</code>

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
--------	-------	--------------

© CVE.report 2021   |

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](#)