



CVE-2021-36310

Published on: 11/19/2021 12:00:00 AM UTC

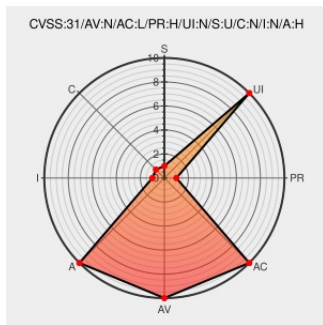
Last Modified on: 11/23/2021 06:49:00 PM UTC

CVE-2021-36310

Source: Mitre

Source: Nist

Print: PDF



Certain versions of **Networking Os10** from **Dell** contain the following vulnerability:

Dell Networking OS10, versions 10.4.3.x, 10.5.0.x, 10.5.1.x & 10.5.2.x, contain an uncontrolled resource consumption flaw in its API service. A high-privileged API user may potentially exploit this vulnerability, leading to a denial of service.

CVE-2021-36310 has been assigned by secure@dell.com to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: **Dell - Networking OS** version < OS10 10.4.3.8, OS10 10.5.0.6C3, OS10 10.5.0.10, OS10 10.5.1.10, OS10 10.5.2.8, OS10 10.5.3.0P1, OS10 10.5.2.3kcc

CVSS3 Score: **4.9 - MEDIUM**

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

CVSS2 Score: **6.8 - MEDIUM**

| Access Vector | Access Complexity | Authentication |
|------------------------|-------------------|---------------------|
| NETWORK | LOW | SINGLE |
| Confidentiality Impact | Integrity Impact | Availability Impact |
| NONE | NONE | COMPLETE |

CVE References

| Description | Tags | Link |
|---------------|--|---|
| Access Denied | www.dell.com text/html | MISC www.dell.com/support/kbdoc/en-us/000193076 |

Inactive Link Not Archived

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 |
|------------------|----------------------|---------------------------------|---------|--------|---------|----------|
| Operating System | Dell | Networking Os10 | All | All | All | All |

cpe:2.3:o:dell:networking_os10:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

| Source | Title | Posted (UTC) |
|----------------------------|--|---------------------|
| @omokazuki | SIOSセキュリティブログを更新しました。Linux Kernelの脆弱性(CVE-2021-36310, CVE-2021-36311, CVE-2021-36312, CVE-2021-36312) #sios_tech... twitter.com/i/web/status/1... | 2021-04-07 19:49:00 |
| @CVEreport | CVE-2021-36310 : Dell Networking OS10, versions 10.4.3.x, 10.5.0.x, 10.5.1.x & 10.5.2.x, contain an uncontrolled re... twitter.com/i/web/status/1... | 2021-11-20 01:46:59 |

[← Previous ID](#)

[Next ID →](#)

© [CVE.report](#) 2022 [Twitter](#) [N](#) |

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](#)