



CVE-2019-12123

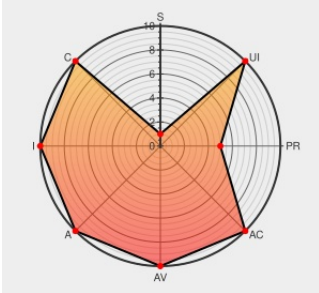
Published on: 03/18/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:40 PM UTC

CVE-2019-12123

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

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



Certain versions of [Open Network Automation Platform](#) from [Onap](#) contain the following vulnerability:

An issue was discovered in ONAP SDNC before Dublin. By executing `sla/printAsXml` with a crafted module parameter, an authenticated user can execute an arbitrary command. All SDC setups that include `admportal` are affected.

CVE-2019-12123 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **8.8 - HIGH**

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

CVSS2 Score: **6.5 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
[OJSI-42] SDNC service allows for arbitrary code execution in <code>sla/printAsXml</code> form (CVE-2019-12123) - ONAP	Exploit Patch Vendor Advisory jira.onap.org text/html	MISC jira.onap.org/browse/OJSI-42

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	Onap	Open Network Automation Platform	All	All	All	All
Application	Onap	Open Network Automation Platform	All	All	All	All
cpe:2.3:a:onap:open_network_automation_platform:*:*:*:*:*:						
cpe:2.3:a:onap:open_network_automation_platform:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→