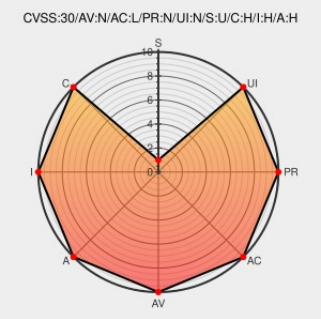
CVE-2019-1010245

Published on: 07/19/2019 12:00:00 AM UTC

Last Modified on: 07/21/2021 11:39:00 AM UTC

CVE-2019-1010245

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



Certain versions of Open Network Operating System from Linuxfoundation contain the following vulnerability:

The Linux Foundation ONOS SDN Controller 1.15 and earlier versions is affected by: Improper Input Validation. The impact is: A remote attacker can execute arbitrary commands on the controller. The component is: apps/yang/src/main/java/org/onosproject/yang/impl/YangLiveCompilerManager.java. The attack vector is: network connectivity. The fixed version is: 1.15.

CVE-2019-1010245 has been assigned by cve-assign@distributedweaknessfiling.org to track the vulnerability - currently rated as CRITICAL severity.

Affected Vendor/Software: **The Linux Foundation** - **ONOS SDN Controller** version **1.15 and earlier versions [fixed: 1.15]**

CVSS3 Score: 9.8 - CRITICAL

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

CVSS2 Score: 7.5 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
onos.pdf - Google Drive	Exploit Third Party Advisory web.archive.org text/html Inactive Link Not Archived	MISC drive.google.com/open?id=1OkMtrMgjjINsDUQwxpGxjbATB6hiwqyv
Gerrit Code Review	Patch Third Party Advisory gerrit.onosproject.org text/html	MISC gerrit.onosproject.org/#/c/20767/

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	Linuxfoundation	Open Network Operating System	All	All	All	All

cpe:2.3:o:linuxfoundation:open_network_operating_system:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

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