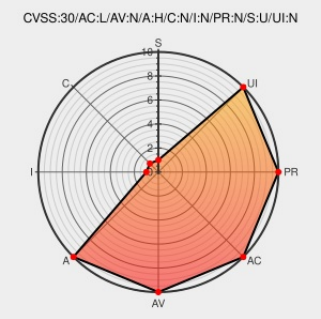
CVE-2019-19627

Published on: 12/06/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:54 PM UTC

CVE-2019-19627

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



Certain versions of Sros2 from Ros contain the following vulnerability:

SROS 2 0.8.1 (after CVE-2019-19625 is mitigated) leaks ROS 2 node-related information regardless of the rtps_protection_kind configuration. (SROS2 provides the tools to generate and distribute keys for Robot Operating System 2 and uses the underlying security plugins of DDS from ROS 2.)

CVE-2019-19627 has been assigned by cve@mitre.org to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 5.3 - MEDIUM

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

CVSS2 Score: 5 - MEDIUM

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

CVE References

Description	Tags	Link
GitHub - ros-swg/turtlebot3_demo: Repository to build and test Turtlebot3 packages	Third Party Advisory, github.com, text/html	MISC github.com/ros-swg/turtlebot3_demo
RVD#922: SROS2 leaks node information · Issue #922 ·	Exploit	MISC

aliasrobotics/RVD · GitHub	Third Party Advisory github.com text/html	github.com/aliasrobotics/RVD/issues/922
SROS2 leaks node information, regardless of rtps_protection_kind setup · Issue #172 · ros2/sros2 · GitHub	Third Party Advisory github.com text/html	MISC github.com/ros2/sros2/issues/172
ROS2 Security workshop | ROSCon 2019	Vendor Advisory ros-swg.github.io text/html	MISC ros-swg.github.io/ROSCon19_Security_Workshop/
SROS2 leaks node information, regardless of rtps_protection_kind setup - asciinema	Third Party Advisory asciinema.org text/html	MISC asciinema.org/a/yuGkBlaPC33wqL4qABRlgxBkd

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	Ros	Sros2	0.8.1	All	All	All
Application	Ros	Sros2	0.8.1	All	All	All

cpe:2.3:a:ros:sros2:0.8.1:*:*:*:*:*:*:*:

cpe:2.3:a:ros:sros2:0.8.1:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→