

New issue

Jump to bottom

RVD#2557: Hardcoded Credentials on MiRX00 Control Dashboard #2557

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: critical 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: 2557
title: 'RVD#2557: Hardcoded Credentials on MiRX00 Control Dashboard'
type: vulnerability
description: Out of the wired and wireless interfaces within MiR100, MiR200 and other vehicles from the MiR fleet, it's possible to access the Control Dashboard on a hardcoded IP address. Credentials to such wireless interface default to well known and widely spread users (omitted) and passwords (omitted). This information is also available in past User Guides and manuals which the vendor distributed. This flaw allows cyber attackers to take control of the robot remotely and make use of the default user interfaces MiR has created, lowering the complexity of attacks and making them available to entry-level attackers. More elaborated attacks can also be established by clearing authentication and sending network requests directly. We have confirmed this flaw in MiR100 and MiR200 but according to the vendor, it might also apply to MiR250, MiR500 and MiR1000.
cwe: CWE-798
cve: CVE-2020-10270
keywords:
- MiR100, MiR200, MiR500, MiR250, MiR1000, ER200, ER-Lite, ER-Flex, ER-One, UVD, Authentication
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: 10.0
  rvss-vector: RVSS:1.0/AV:AN/AC:L/PR:L/UI:N/Y:Z/S:U/C:H/I:H/A:H/H:H
  severity-description: Critical
  cvss-score: 9.8
  cvss-vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
links:
- https://cwe.mitre.org/data/definitions/798.html
- https://www.mobile-industrial-robots.com/media/2714/mir100-user-guide_robot-interface-20-v10.pdf
- http://bernharddieber.com/publication/taurer2019mirsafety
- https://github.com/aliasrobotics/RVD/issues/2557
flaw:
  phase: runtime-operation
  specificity: general-issue
  architectural-location: Platform code
  application: All
  subsystem: UI:Login
  package: N/A
  languages: None
  date-detected: 2019-07-01
  detected-by: Alias Robotics (https://aliasrobotics.com/)
  detected-by-method: testing dynamic, web browser.
  date-reported: '2020-06-24'
  reported-by: "Victor Mayoral Vilches (Alias Robotics)"
  reported-by-relationship: security researcher
  issue: https://github.com/aliasrobotics/RVD/issues/2557
  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:latest
        - volume: registry.gitlab.com/aliasrobotics/offensive/alurity/expl_robotsploit: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: echo "Waiting until the dashboard launches..."; sleep 10
          - command: 'robotsploit -m exploits/mir/dashboard/http_default_creds -s "target $TARGET" '
    - container:
```

```
- name: mir100
- window:
  - name: setup
  - commands:
    - command: mkdir /var/run/ssh
    - command: /usr/sbin/ssh
    - 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: 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: critical vendor: Easy Robotics vendor: Enabled Robotics vendor: Mobile Industrial Robots vendor: UVD Robots vulnerability labels on Jun 24, 2020

 **rvd-bot** changed the title ~~Hardcoded Credentials on MiRX00 Control Dashboard~~ **RVD#2557: Hardcoded Credentials on MiRX00 Control Dashboard** 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: critical 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

