DEFENSIVE AND OFFENSIVE
ROBOT SECURITY

ENDIKA GIL URIARTE
dendika@aliasrobotics.com

VÍCTOR MAYORAL VILCHES
victor@aliasrobotics.com

ALIAS ROBOTICS
Robot Cybersecurity
OFFENSIVE ROBOT SECURITY

CVE-2019-14899
INFERRING AND HIJACKING VPN-TUNNELED TCP CONNECTIONS.
04 DEC 2019 19:37:07 -0700
ALIAS’ ATTACKER MODEL

**EXTERNAL**
- Reconnaissance
  - Footprinting
  - Fingerprinting
- Weaponization
  - Targeting
  - Testing (dyn. or static)
- Cyber intrusion
  - Delivery
  - Exploitation
- Privilege escalation

**INTERNAL**
- Privilege escalation
- Cyber intrusion
- Weaponization
- Reconnaissance
- Lateral movement
- Exfiltration
- Control
DEFINING FLAWS

**BUG** (security)

An error, flaw, failure or fault in a computer program or system that causes it to produce an **incorrect or unexpected result**, or to behave in unintended ways.


**WEAKNESS**

**Bug** that **can** lead to software vulnerabilities.

MITRE, CWE, https://cwe.mitre.org/about/faq.html#A.2

**VULNERABILITY**

A **weakness** in software that can be **directly used by a hacker** to gain access to a system or network.

MITRE, CWE, https://cwe.mitre.org/about/faq.html#A.2

**0-DAY**

Vulnerability that is **unknown to, or unaddressed by**, those who should be interested in mitigating the vulnerability.

VULNERABILITY MITIGATION AND 0-DAYS

DAYS UNTIL MITIGATION OR UNTIL TODAY

0-DAYS PROPORTION

Data from Robot Vulnerability Database (RVD), https://github.com/aliasrobotics/RVD, removed tickets in triage for ROS, ROS2 and UR

Data from Robot Vulnerability Database (RVD), https://github.com/aliasrobotics/RVD, removed tickets in triage for ROS, ROS2 and UR
## VULNERABILITY LANDSCAPE

### ROBOT VULNERABILITY DATABASE (RVD)

<table>
<thead>
<tr>
<th></th>
<th>OPEN</th>
<th>CLOSED</th>
<th>ALL</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>VULNERABILITIES</strong></td>
<td>Vulnerabilities 102</td>
<td>Vulnerabilities 8</td>
<td>Vulnerabilities 110</td>
</tr>
<tr>
<td><strong>BUGS</strong></td>
<td>Bugs 79</td>
<td>Bugs 191</td>
<td>Bugs 270</td>
</tr>
<tr>
<td><strong>OTHERS</strong></td>
<td>Others 0</td>
<td>Others 1</td>
<td>Others 1</td>
</tr>
</tbody>
</table>

### VULNERABILITIES (OPEN)

<table>
<thead>
<tr>
<th>Vulnerability Type</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vuln.Critical</td>
<td>23</td>
</tr>
<tr>
<td>Vuln.High</td>
<td>23</td>
</tr>
<tr>
<td>Vuln.Medium</td>
<td>12</td>
</tr>
<tr>
<td>Vuln.Low</td>
<td>1</td>
</tr>
</tbody>
</table>

Last updated Fri, 06 Dec 2019 23:40:48 GMT

Robot Vulnerability Database (RVD), [https://github.com/aliasrobotics/RVD](https://github.com/aliasrobotics/RVD)
VULNERABILITY LANDSCAPE

SEVERITY IN OPEN TICKETS
BY MANUFACTURER

VULNERABILITIES
BY VENDOR (PUBLIC)

Data from Robot Vulnerability Database (RVD), https://github.com/aliasrobotics/RVD.
## VULNERABILITY LANDSCAPE FOR ROS

### CWE-200
- Information Exposure

### CWE-340
- Predictability Problems

### CWE-327
- Use of a Broken or Risky Cryptographic Algorithm

### CWE-208
- Information Exposure Through Timing Discrepancy

### None
- N/A, generally needs further research

### CWE-686
- Reliance on Security Through Obscurity

### CWE-359
- Exposure of Private Information (‘Privacy Violation’)

### VULNERABILITY LANDSCAPE FOR ROS2

<table>
<thead>
<tr>
<th>CWE</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CWE-300</td>
<td>Channel Accessible by Non-Endpoint (‘Man-in-the-Middle’)</td>
</tr>
<tr>
<td>None</td>
<td>N/A, generally needs further research</td>
</tr>
<tr>
<td>CWE-400</td>
<td>Uncontrolled Resource Consumption</td>
</tr>
<tr>
<td>CWE-306</td>
<td>Missing Authentication for Critical Function</td>
</tr>
<tr>
<td>CWE-924</td>
<td>Improper Enforcement of Message Integrity During Transmission in a C...</td>
</tr>
</tbody>
</table>

Data from Robot Vulnerability Database (RVD),
https://github.com/aliasrobotics/RVD.
VULNERABILITY EXPLOITATION

CVE-2019-19625:
SROS2 leaks node information
CVE-2019-19625: SROS2 leaks node information

Networks:
- network:
  - driver: overlay
  - name: net1
  - encryption: false

Containers:
- container:
  - name: subject1
  - modules:
    - base:
      - registry.gitlab.com/aliasrobotics/offensive/alurity/ros2/ros2:latest
      - network: net1

- container:
  - name: subject2
  - modules:
    - base:
      - registry.gitlab.com/aliasrobotics/offensive/alurity/ros2/ros2:latest
      - volume:
        - registry.gitlab.com/aliasrobotics/offensive/alurity/deve_atom
      - network: net1

- container:
  - name: attacker
  - modules:
    - base:
      - registry.gitlab.com/aliasrobotics/offensive/alurity/ros2/ros2:latest
      - volume:
        - registry.gitlab.com/aliasrobotics/offensive/alurity/reco_aztnara
      - network: net1
MODULAR AND COMPOSABLE, FOR ROBOTS

 TOOLBOX FOR
 ROBOT SECURITY

alurity
# a simple configuration for a UR3 subject

```
ur3:
  - modules:
    - base: alurity:latest # base module
    - volume: comp_ros:kinetic
    - volume: robo_ur3:latest
    - volume: comp_moveit:latest
    - volume: reco_aztarna:latest
    - volume: expl_robosploit:latest
    - volume: fore_bbtools:latest
    - volume: deve_rviz:latest
    - volume: deve_gazebo:latest
    - network: bridge
```

TOOLBOX FOR ROBOT SECURITY

>ALURITY.YAML

ALURITY

MOVEIT

AZTARNA

ROBOSPLOIT

BBTOOLS

RVIZ

GAZEBO

UR3 SUBJECT IMAGE

PERFORM RECONNAISSANCE

UR3

MOVEIT

SOLUTION ALURITY
SOLUTION
ALURITY

TOOLBOX FOR ROBOT SECURITY

ALURITY

LOCAL NETWORK 10.0.0.0/24

VXLAN

UR3 SUBJECT IMAGE
PERFORM RECONNAISSANCE

ATTACK IMAGE
PERFORM RECONNAISSANCE

ROS

UR3

MOVEIT

AZTARNA

ROBOSPLOIT

BBTOOLS

RVIZ

GAZEBO

ROS

UR3

MOVEIT

ROBOSPLOIT

ROSCHAOS

METASPLOIT

GOOGLE SANITIZERS

CPPCHECK

WIRESHARK

AZTARNA
ALURITY

SOLUTION

TOOLBOX FOR ROBOT SECURITY
A STUDY CASE
AKERBELTZ
ROBOT RANSOMWARE
ADDED VALUE OF ALIAS ROBOTICS

CASE OF STUDY
UNIVERSAL ROBOTS

- Publicly available
- Discovered by Alias Robotics (private)
- All (known) vulnerabilities
DEFENSIVE ROBOT SECURITY
COMING SOON
INTRODUCING RIS FOR UNIVERSAL ROBOTS

| Hardens / Mitigates known vulnerabilities in Universal Robots |

| Alerts / Prevents of threats to Universal Robots |

NORMAL: No problem status
WARNING: Anomaly with potential threat to the system
DANGER: Dangerous action possibly compromising the system
INTRODUCING RIS FOR UNIVERSAL ROBOTS

Enable or disable alert Popups. Activate it if you want to receive notifications when alerts occur.

Check your UR robot's last alerts. It shows all recent Danger or Warning alerts that have not been checked.

Reset to a no problem status when you have already checked your alerts.

Contains information about RIS operation. Come here whenever you need help.
MOTIVATION

ROBOT SECURITY SURVEY

(DISTINGUISHED) ROBOT MANUFACTURER QUOTES

“Security... yes, we hold PLD (and start safety pitch) blah”

“Cybersecurity flaws greatly facilitate system integration”

“We know our robots have a set of reported vulnerabilities
- We leave solving those up to the end user”

- Upon PoC attack “This is not hacking a robot... You are trying to drum up business to sell your consultancy services”

- Upon Vulnerability advisory: “Do not connect your robot”

“Every thing will be fixed in the next release”... 3 months later... “it can’t be fixed”

“Cybersecurity is up to the robot user hacker”
A SNEAK PEAK INTO ROBOT SECURITY SURVEY

OBJECTIVE

Depict a global landscape of the current security situation in robotics.

RATIONALE

The need to assess precisely the security concerns in the robotics value chain and the strategies of cybersecurity so far.
STRUCTURE
ROBOT SECURITY SURVEY

1. General Questions and background
2. Robot usage and application
3. Cybersecurity specifics
4. Standardization Items
RESPONDANT PROFILES

43 RESPONSES
AT TIME OF WRITING

RESPONDANT PROFILES

- University: 34.07%
- Robot manufacturer: 17.08%
- Other: 9.79%
- Hardware components: 2.40%
- Research Transfer: 9.79%
- Integrator: 4.90%
- Robot End-user: 9.79%
- Software component: 12.19%

VARIOUS BACKGROUNDS & POSITIONS

- R&D: 24%
- Software Engineer: 26%
- Electrical Engineer: 9.50%
- CEO: 7.10%
- Management (CTO): 11.90%
- Security Engineer: 7.10%
- User: 4.80%
- Sales and marketing: 4.80%
- Test Engineer: 2.40%
- Mechanical Engineer: 2.40%

VARIOUS BACKGROUNDS & POSITIONS

- Robot End-user: 9.79%
- University: 34.07%
- Other: 9.79%
- Hardware components: 2.40%
- Research Transfer: 9.79%
- Integrator: 4.90%
- Software component: 12.19%
(IN)SECURITY OBSERVATIONS

51% IDENTIFIED CYBER - WEAKNESSES IN ROBOTS

9% WITNESSED A CYBERATTACK

1 EXPOSED NETWORK SERVICES

2 POTENTIAL PHYSICAL ATTACKS

3 ISSUES IN FIRMWARE

1 SUSPECTED/OBSERVED VULNERABILITIES
(IN)SECURITY CONCERNS

**RESPONDENT FEARS**

1st: IP STEALING
2nd: SAFETY VIOLATIONS

**OUTCOME LIKELIHOOD**

1st: SAFETY VIOLATIONS
2nd: DATA LOSS

**MALICIOUS ACTORS**

1st: HACKERS
2nd: UNINTENTIONAL EMPLOYEES
SECURITY PERCEPTION

8/10

2.2/10

SECURITY RELEVANCE

PROTECTED AS AN ENDPOINT?

UNSTACKED
RELEVANCE & ENDPOINT SECURITY

Security relevance

Robot protected as an endpoint

Large Enterprise
RTO
SME
Startup
University
ECONOMIC CONSIDERATIONS

73% OPEN TO INVEST

26% HAVE ACTUALLY INVESTED

73% THINK THEY HAVE NOT INVESTED ENOUGH
CALL FOR ACTION
REMOVING 0-DAYS FROM ROBOTICS