

New issue

Jump to bottom

RVD#1489: Unprotected intellectual property in Universal Robots controller CB 3.1 across firmware versions #1489

Open rvd-bot opened this issue on Apr 3, 2020 · 2 comments

Labels CVE-2020-10267 CWE-311 robot component: Universal Robots Controller robot: UR3 robot: UR5 robot: UR10 severity: high vendor: Universal Robots vulnerability

rvd-bot commented on Apr 3, 2020 • edited by vmayoral

Contributor

```
{
  "id": 1489,
  "title": "RVD#1489: Unprotected intellectual property in Universal Robots controller CB 3.1 across firmware versions",
  "type": "vulnerability",
  "description": "Universal Robots control box CB 3.1 across firmware versions (tested on 3.13.0, 3.12.1, 3.12, 3.11 and 3.10.0) does not encrypt or protect in any way the intellect",
  "cwe": "CWE-311 (Missing Encryption of Sensitive Data)",
  "cve": "CVE-2020-10267",
  "keywords": [
    "Universal Robots"
  ],
  "system": "UR3, UR5 and UR10",
  "vendor": "Universal Robots",
  "severity": {
    "rvss-score": 6.5,
    "rvss-vector": "RVSS:1.0/AV:AN/AC:L/PR:N/UI:N/Y:Z/S:U/C:H/I:N/A:N/H:N",
    "severity-description": "high",
    "cvss-score": 7.5,
    "cvss-vector": "CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N"
  },
  "links": [
    "https://www.universal-robots.com/plus/",
    "https://github.com/aliasrobotics/RVD/issues/1489"
  ],
  "flaw": {
    "phase": "testing",
    "specificity": "general issue",
    "architectural-location": "platform code",
    "application": "industrial robot manipulator",
    "subsystem": "manipulation:actuation",
    "package": "libc6 2.19-11 i386",
    "languages": "C",
    "date-detected": null,
    "detected-by": "V\u000edctor Mayoral Vilches <victor@aliasrobotics.com>",
    "detected-by-method": "testing",
    "date-reported": "2020-04-03",
    "reported-by": "V\u000edctor Mayoral Vilches <victor@aliasrobotics.com>",
    "reported-by-relationship": "security researcher",
    "issue": "https://github.com/aliasrobotics/RVD/issues/1489",
    "reproducibility": "always",
    "trace": "N/A",
    "reproduction": "https://asciinema.org/a/EJ5ZzqAbiVvPlyNABXyOk3iez",
    "reproduction-image": "Not available"
  },
  "exploitation": {
    "description": "Since URCaps aren't secured, its extraction requires attackers to access the file system (remotely or locally) and extract it from '/root/.urcaps/' folder. Res",
    "exploitation-image": "Not available",
    "exploitation-vector": "Not available"
  },
  "mitigation": {
    "description": "Use a combination of digital encryption and signatures to protect installed intellectual property. Ensure that file system where these file reside is read-only",
    "pull-request": "Not available",
    "date-mitigation": null
  }
}
```

rvd-bot added severity: high vendor: Universal Robots vulnerability labels on Apr 3, 2020

rvd-bot changed the title Unprotected intellectual property in Universal Robots controller CB 3.1 across firmware versions RVD#1489: Unprotected intellectual property in Universal Robots controller CB 3.1 across firmware versions on Apr 3, 2020

vmayoral commented on Apr 3, 2020

Member

Demonstration available at <https://asciinema.org/a/EJ5ZzqAbiVvPlyNABXyOk3iez>

Reproduction simplified with the following alurity.yml file:

Details

vmayoral added robot: UR10 robot: UR3 robot: UR5 robot component: Universal Robots Controller CVE-2020-10267 CWE-311 labels on Apr 3, 2020

vmayoral commented on Apr 4, 2020

Member

Assigned CVE ID.

Assignees

No one assigned

Labels

CVE-2020-10267 CWE-311 robot component: Universal Robots Controller robot: UR3 robot: UR5 robot: UR10 severity: high vendor: Universal Robots vulnerability

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants

