



CVE-2020-10277

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2020-10277
State	PUBLIC
Assigner	cve@aliasrobotics.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-06-24 05:15:00 UTC
Updated	2021-09-14 17:20:00 UTC
Description	There is no mechanism in place to prevent a bad operator to boot from a live OS image, this can lead to extraction of sensil

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Easyrobotics	Er-flex	-	All	All	All
Hardware	Easyrobotics	Er-flex	-	All	All	All
Operating System	Easyrobotics	Er-flex Firmware	-	All	All	All
Operating System	Easyrobotics	Er-flex Firmware	-	All	All	All
Hardware	Easyrobotics	Er-lite	-	All	All	All
Hardware	Easyrobotics	Er-lite	-	All	All	All
Operating System	Easyrobotics	Er-lite Firmware	-	All	All	All
Operating System	Easyrobotics	Er-lite Firmware	-	All	All	All
Hardware	Easyrobotics	Er-one	-	All	All	All
Hardware	Easyrobotics	Er-one	-	All	All	All
Operating System	Easyrobotics	Er-one Firmware	-	All	All	All
Operating System	Easyrobotics	Er-one Firmware	-	All	All	All
Hardware	Easyrobotics	Er200	-	All	All	All
Hardware	Easyrobotics	Er200	-	All	All	All
Operating System	Easyrobotics	Er200 Firmware	-	All	All	All
Operating System	Easyrobotics	Er200 Firmware	-	All	All	All
Hardware	Mobile-industrial-robots	Mir100	-	All	All	All

Hardware	Mobile-industrial-robots	Mir100	-	All	All	All
Hardware	Mobile-industrial-robots	Mir1000	-	All	All	All
Hardware	Mobile-industrial-robots	Mir1000	-	All	All	All
Operating System	Mobile-industrial-robots	Mir1000 Firmware	-	All	All	All
Operating System	Mobile-industrial-robots	Mir1000 Firmware	-	All	All	All
Operating System	Mobile-industrial-robots	Mir100 Firmware	All	All	All	All
Hardware	Mobile-industrial-robots	Mir200	-	All	All	All
Hardware	Mobile-industrial-robots	Mir200	-	All	All	All
Operating System	Mobile-industrial-robots	Mir200 Firmware	-	All	All	All
Operating System	Mobile-industrial-robots	Mir200 Firmware	-	All	All	All
Hardware	Mobile-industrial-robots	Mir250	-	All	All	All
Hardware	Mobile-industrial-robots	Mir250	-	All	All	All
Operating System	Mobile-industrial-robots	Mir250 Firmware	-	All	All	All
Operating System	Mobile-industrial-robots	Mir250 Firmware	-	All	All	All
Hardware	Mobile-industrial-robots	Mir500	-	All	All	All
Hardware	Mobile-industrial-robots	Mir500	-	All	All	All
Operating System	Mobile-industrial-robots	Mir500 Firmware	-	All	All	All
Operating System	Mobile-industrial-robots	Mir500 Firmware	-	All	All	All
Hardware	Uvd-robots	Uvd	-	All	All	All
Hardware	Uvd-robots	Uvd	-	All	All	All
Operating System	Uvd-robots	Uvd Firmware	-	All	All	All
Operating System	Uvd-robots	Uvd Firmware	-	All	All	All

References

Reference

RVD#2562: Booting from a live image leads to exfiltration of sensible information and privilege escalation · Issue #2562 · aliasrobotics/RVD · C

CVE Program record

NVD vulnerability detail

Vendor Comments And Credit

Discovery Credit

LEGACY: Lander Usategui, Alfonso Glera (Alias Robotics)

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)