



Command injection in Dashboard Server interface

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

CVE	CVE-2026-8153
State	PUBLISHED
Assigner	TRO
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-08 12:16:29 UTC
Updated	2026-05-11 10:16:15 UTC
Description	OS command injection in Dashboard Server interface in Universal Robots PolyScope versions prior to 5.25.1 allows unauth

Risk And Classification

Primary CVSS: v3.1 9.8 CRITICAL from 1b7e193f-2525-49a1-b171-84af8827c9eb

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

EPSS: 0.010910000 probability, percentile 0.780910000 (date 2026-05-12)

Problem Types: CWE-78 | CWE-78 CWE-78 Improper neutralization of special elements used in an OS command ('OS command injection')

Version	Source	Type	Score	Severity	Vector
3.1	1b7e193f-2525-49a1-b171-84af8827c9eb	Secondary	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
3.1	CNA	CVSS	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

ntegrity

High

Availability

High

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Universal Robots	PolyScope 5	affected 5.25.1 semver	Not specified

References

Reference	Source	Link
www.universal-robots.com/developer/communication-protocol/dashboard-server	1b7e193f-2525-49a1-b171-84af8827c9eb	www.universal-robots.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

Vendor Comments And Credit

Discovery Credit

CNA: Vera Mens of Claroty Team82 (en)

Additional Advisory Data

Solutions

CNA: Update to version 5.25.1 or later, or disable Dashboard Server interface

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