



CVE-2023-43803

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

Summary

CVE	CVE-2023-43803
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-10-18 21:15:00 UTC
Updated	2023-11-08 13:15:00 UTC
Description	Arduino Create Agent is a package to help manage Arduino development. This vulnerability affects the endpoint <code>`v2/pkgst</code>

Risk And Classification

Problem Types: CWE-22

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Arduino	Create Agent	All	All	All	All

References

Reference	Source	Link	Tags
Path traversal - arbitrary file deletes · Advisory · arduino/arduino-create-agent · GitHub	MISC	github.com	
Release 1.3.3 · arduino/arduino-create-agent · GitHub	MISC	github.com	
New Vulnerabilities in Arduino Software Allow Privilege Escalation	MISC	www.nozominetworks.com	
[SECURITY] [DLA 3649-1] python-urllib3 security update		lists.debian.org	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[6000284](#) Debian Security Update for python-urllib3 (DLA 3649-1)

[995624](#) GO (Go) Security Update for github.com/arduino/arduino-create-agent (GHSA-m5jc-r4gf-c6p8)

© [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](#).

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