



CVE-2021-32561

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

Summary

CVE	CVE-2021-32561
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-05-11 14:15:00 UTC
Updated	2021-05-26 19:42:00 UTC
Description	OctoPrint before 1.6.0 allows XSS because API error messages include the values of input parameters.

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Octoprint	Octoprint	All	All	All	All

References

Reference	Source	Link	Tags
OctoPrint.org - New release: 1.6.0	MISC	octoprint.org	
Jakub Brzozowski	MISC	www.brzozowski.io	
The (in)secure story of OctoPrint - Cybersecurity and research blog	MISC	www.brzozowski.io	
Release 1.6.0 · OctoPrint/OctoPrint · GitHub	MISC	github.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

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

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