



CVE-2020-10670

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

Summary

CVE	CVE-2020-10670
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-03-19 19:15:00 UTC
Updated	2020-03-23 17:03:00 UTC
Description	The web application exposed by the Canon Oce Colorwave 500 4.0.0.0 printer is vulnerable to Reflected XSS in the param

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Canon	Oce Colorwave 500	-	All	All	All
Hardware	Canon	Oce Colorwave 500	-	All	All	All
Operating System	Canon	Oce Colorwave 500 Firmware	All	All	All	All

References

Reference

- Oce Colorwave 500 CSRF / XSS / Authentication Bypass ≈ Packet Storm
- Hacking the Oce Colorwave printer: when a quick security assessment determines the success of a Red Team exercise. - Red Timmy Security
- CVE Program record
- NVD vulnerability detail

No vendor comments have been submitted for this CVE.

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

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](#)