



CVE-2022-43608

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

Summary

CVE	CVE-2022-43608
State	PUBLIC
Assigner	zdi-disclosures@trendmicro.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-03-29 19:15:00 UTC
Updated	2023-04-08 01:56:00 UTC
Description	This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of Canon imageCLAS

Risk And Classification

Problem Types: CWE-190

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Canon	Mf644cdw	-	All	All	All
Operating System	Canon	Mf644cdw Firmware	10.03	All	All	All

References

Reference	Source
Vulnerability Mitigation /Remediation Against Buffer Overflow for Laser Printers and Small Office Multifunction Printers - Canon PSIRT	MISC
ZDI-22-1666 Zero Day Initiative	MISC
CVE Program record	CVE
NVD vulnerability detail	NVD

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