



CVE-2022-41798

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

Summary

CVE	CVE-2022-41798
State	PUBLIC
Assigner	vultures@jpcert.or.jp
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-12-05 04:15:00 UTC
Updated	2022-12-06 16:42:00 UTC
Description	Session information easily guessable vulnerability exists in Kyocera Document Solutions MFPs and printers, which may allow

Risk And Classification

Problem Types: CWE-290

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Kyocera	Ecosys M2535dn	-	All	All	All
Operating System	Kyocera	Ecosys M2535dn Firmware	-	All	All	All
Hardware	Kyocera	Ecosys M6526cdn	-	All	All	All
Operating System	Kyocera	Ecosys M6526cdn Firmware	-	All	All	All
Hardware	Kyocera	Ecosys M6526cidn	-	All	All	All
Operating System	Kyocera	Ecosys M6526cidn Firmware	-	All	All	All
Hardware	Kyocera	Ecosys P2135dn	-	All	All	All
Operating System	Kyocera	Ecosys P2135dn Firmware	-	All	All	All
Hardware	Kyocera	Ecosys P4040dn	-	All	All	All
Operating System	Kyocera	Ecosys P4040dn Firmware	-	All	All	All
Hardware	Kyocera	Ecosys P6026cdn	-	All	All	All
Operating System	Kyocera	Ecosys P6026cdn Firmware	-	All	All	All
Hardware	Kyocera	Fs-1370dn	-	All	All	All
Operating System	Kyocera	Fs-1370dn Firmware	-	All	All	All
Hardware	Kyocera	Fs-c2026mfp	-	All	All	All
Operating System	Kyocera	Fs-c2026mfp Firmware	-	All	All	All
Hardware	Kyocera	Fs-c2126mfp	-	All	All	All

Hardware	Kyocera	Fs-c2126mfp	-	All	All	All
Operating System	Kyocera	Fs-c2126mfp Firmware	-	All	All	All
Operating System	Kyocera	Fs-c2126mfp Firmware	-	All	All	All
Hardware	Kyocera	Fs-c5250dn	-	All	All	All
Operating System	Kyocera	Fs-c5250dn Firmware	-	All	All	All
Hardware	Kyocera	Ls-1035mfp	-	All	All	All
Operating System	Kyocera	Ls-1035mfp Firmware	-	All	All	All
Hardware	Kyocera	Ls-1135mfp	-	All	All	All
Operating System	Kyocera	Ls-1135mfp Firmware	-	All	All	All
Hardware	Kyocera	Ls-2100dn	-	All	All	All
Operating System	Kyocera	Ls-2100dn Firmware	-	All	All	All
Hardware	Kyocera	Ls-3140mfp	-	All	All	All
Hardware	Kyocera	Ls-3140mfp	-	All	All	All
Operating System	Kyocera	Ls-3140mfp Firmware	-	All	All	All
Operating System	Kyocera	Ls-3140mfp Firmware	-	All	All	All
Hardware	Kyocera	Ls-3640mfp	-	All	All	All
Operating System	Kyocera	Ls-3640mfp Firmware	-	All	All	All
Hardware	Kyocera	Ls-4200dn	-	All	All	All
Operating System	Kyocera	Ls-4200dn Firmware	-	All	All	All
Hardware	Kyocera	Ls-4300dn	-	All	All	All
Operating System	Kyocera	Ls-4300dn Firmware	-	All	All	All
Hardware	Kyocera	Ls-c8600dn	-	All	All	All
Operating System	Kyocera	Ls-c8600dn Firmware	-	All	All	All
Hardware	Kyocera	Ls-c8650dn	-	All	All	All
Operating System	Kyocera	Ls-c8650dn Firmware	-	All	All	All
Hardware	Kyocera	Taskalfa 205c	-	All	All	All
Operating System	Kyocera	Taskalfa 205c Firmware	-	All	All	All
Hardware	Kyocera	Taskalfa 206ci	-	All	All	All
Operating System	Kyocera	Taskalfa 206ci Firmware	-	All	All	All
Hardware	Kyocera	Taskalfa 255	-	All	All	All
Hardware	Kyocera	Taskalfa 255c	-	All	All	All
Operating System	Kyocera	Taskalfa 255c Firmware	-	All	All	All
Operating System	Kyocera	Taskalfa 255 Firmware	-	All	All	All
Hardware	Kyocera	Taskalfa 256ci	-	All	All	All
Operating System	Kyocera	Taskalfa 256ci Firmware	-	All	All	All

Hardware	Kyocera	Taskalfa 256i	-	All	All	All
Operating System	Kyocera	Taskalfa 256i Firmware	-	All	All	All
Hardware	Kyocera	Taskalfa 305	-	All	All	All
Hardware	Kyocera	Taskalfa 3050ci	-	All	All	All
Operating System	Kyocera	Taskalfa 3050ci Firmware	-	All	All	All
Operating System	Kyocera	Taskalfa 305 Firmware	-	All	All	All
Hardware	Kyocera	Taskalfa 306i	-	All	All	All
Operating System	Kyocera	Taskalfa 306i Firmware	-	All	All	All
Hardware	Kyocera	Taskalfa 3500i	-	All	All	All
Operating System	Kyocera	Taskalfa 3500i Firmware	-	All	All	All
Hardware	Kyocera	Taskalfa 3550ci	-	All	All	All
Operating System	Kyocera	Taskalfa 3550ci Firmware	-	All	All	All
Hardware	Kyocera	Taskalfa 4500i	-	All	All	All
Operating System	Kyocera	Taskalfa 4500i Firmware	-	All	All	All
Hardware	Kyocera	Taskalfa 4550ci	-	All	All	All
Operating System	Kyocera	Taskalfa 4550ci Firmware	-	All	All	All
Hardware	Kyocera	Taskalfa 5500i	-	All	All	All
Operating System	Kyocera	Taskalfa 5500i Firmware	-	All	All	All
Hardware	Kyocera	Taskalfa 5550ci	-	All	All	All
Operating System	Kyocera	Taskalfa 5550ci Firmware	-	All	All	All
Hardware	Kyocera	Taskalfa 6500i	-	All	All	All
Operating System	Kyocera	Taskalfa 6500i Firmware	-	All	All	All
Hardware	Kyocera	Taskalfa 6550ci	-	All	All	All
Operating System	Kyocera	Taskalfa 6550ci Firmware	-	All	All	All
Hardware	Kyocera	Taskalfa 7550ci	-	All	All	All
Operating System	Kyocera	Taskalfa 7550ci Firmware	-	All	All	All
Hardware	Kyocera	Taskalfa 8000i	-	All	All	All
Operating System	Kyocera	Taskalfa 8000i Firmware	-	All	All	All

References

Reference	Source	Link
Security vulnerabilities in our products KYOCERA Document Solutions	MISC	www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html
JVN#46345126: Multiple vulnerabilities in the web interfaces of Kyocera Document Solutions MFPs and printers	MISC	jvn.jp
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

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](#).

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