



CVE-2019-19363

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2019-19363
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-01-24 18:15:00 UTC
Updated	2023-02-10 16:59:00 UTC
Description	An issue was discovered in Ricoh (including Savin and Lanier) Windows printer drivers prior to 2020 that allows attackers to

Risk And Classification

Problem Types: CWE-732

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Ricoh	Generic Pcl5 Driver	-	All	All	All
Application	Ricoh	Generic Pcl5 Driver	-	All	All	All
Application	Ricoh	Pcl6 Pcl XI Driver	-	All	All	All
Application	Ricoh	Pcl6 Driver For Universal Print	All	All	All	All
Application	Ricoh	Pcl6 Driver For Universal Print	All	All	All	All
Application	Ricoh	Pcl6 Pcl XI Driver	-	All	All	All
Application	Ricoh	Pcl6 Pcl XI Driver	-	All	All	All
Application	Ricoh	Pc Fax Generic Driver	-	All	All	All
Application	Ricoh	Pc Fax Generic Driver	-	All	All	All
Application	Ricoh	Postscript3 Driver	-	All	All	All
Application	Ricoh	Postscript3 Driver	-	All	All	All
Application	Ricoh	Ps Driver For Universal Print	All	All	All	All
Application	Ricoh	Ps Driver For Universal Print	All	All	All	All
Application	Ricoh	Rpcs Driver	-	All	All	All
Application	Ricoh	Rpcs Driver	-	All	All	All
Application	Ricoh	Rpcs Raster Driver	-	All	All	All
Application	Ricoh	Rpcs Raster Driver	-	All	All	All

References

Reference	Source
Ricoh Printer Driver Local Privilege Escalation ≈ Packet Storm	MISC
Ricoh Driver Privilege Escalation ≈ Packet Storm	MISC
JVN#15697526: Privilege escalation vulnerability in multiple RICOH printer drivers	JVN
Full Disclosure: CVE-2019-19363 - Local Privilege Escalation in many Ricoh Printer Drivers for Windows	FULLD
Update: Printer Security Program issued to address potential vulnerabilities in some of Ricoh's printer/PC fax drivers Global Ricoh	CONF
CVE Program record	CVE.C
NVD vulnerability detail	NVD

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](#)