



CVE-2021-28671

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

Summary

CVE	CVE-2021-28671
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-03-29 21:15:00 UTC
Updated	2021-04-05 20:21:00 UTC
Description	Xerox Phaser 6510 before 64.65.51 and 64.59.11 (Bridge), WorkCentre 6515 before 65.65.51 and 65.59.11 (Bridge), Versa

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Xerox	Phaser 6510	-	All	All	All
Operating System	Xerox	Phaser 6510 Firmware	All	All	All	All
Hardware	Xerox	Versalink B400	-	All	All	All
Operating System	Xerox	Versalink B400 Firmware	All	All	All	All
Hardware	Xerox	Versalink B405	-	All	All	All
Operating System	Xerox	Versalink B405 Firmware	All	All	All	All
Hardware	Xerox	Versalink B600	-	All	All	All
Operating System	Xerox	Versalink B600 Firmware	All	All	All	All
Hardware	Xerox	Versalink B605	-	All	All	All
Operating System	Xerox	Versalink B605 Firmware	All	All	All	All
Hardware	Xerox	Versalink B610	-	All	All	All
Operating System	Xerox	Versalink B610 Firmware	All	All	All	All
Hardware	Xerox	Versalink B615	-	All	All	All
Operating System	Xerox	Versalink B615 Firmware	All	All	All	All
Hardware	Xerox	Versalink B7025	-	All	All	All
Operating System	Xerox	Versalink B7025 Firmware	All	All	All	All
Hardware	Xerox	Versalink B7030	-	All	All	All

Operating System	Xerox	Versalink B7030 Firmware	All	All	All	All
Hardware	Xerox	Versalink B7035	-	All	All	All
Operating System	Xerox	Versalink B7035 Firmware	All	All	All	All
Hardware	Xerox	Versalink C400	-	All	All	All
Operating System	Xerox	Versalink C400 Firmware	All	All	All	All
Hardware	Xerox	Versalink C405	-	All	All	All
Operating System	Xerox	Versalink C405 Firmware	All	All	All	All
Hardware	Xerox	Versalink C500	-	All	All	All
Operating System	Xerox	Versalink C500 Firmware	All	All	All	All
Hardware	Xerox	Versalink C505	-	All	All	All
Operating System	Xerox	Versalink C505 Firmware	All	All	All	All
Hardware	Xerox	Versalink C600	-	All	All	All
Operating System	Xerox	Versalink C600 Firmware	All	All	All	All
Hardware	Xerox	Versalink C605	-	All	All	All
Operating System	Xerox	Versalink C605 Firmware	All	All	All	All
Hardware	Xerox	Versalink C7000	-	All	All	All
Operating System	Xerox	Versalink C7000 Firmware	All	All	All	All
Hardware	Xerox	Versalink C7020	-	All	All	All
Operating System	Xerox	Versalink C7020 Firmware	All	All	All	All
Hardware	Xerox	Versalink C7025	-	All	All	All
Operating System	Xerox	Versalink C7025 Firmware	All	All	All	All
Hardware	Xerox	Versalink C7030	-	All	All	All
Operating System	Xerox	Versalink C7030 Firmware	All	All	All	All
Hardware	Xerox	Versalink C8000	-	All	All	All
Hardware	Xerox	Versalink C8000w	-	All	All	All
Operating System	Xerox	Versalink C8000w Firmware	All	All	All	All
Operating System	Xerox	Versalink C8000 Firmware	All	All	All	All
Hardware	Xerox	Versalink C9000	-	All	All	All
Operating System	Xerox	Versalink C9000 Firmware	All	All	All	All
Hardware	Xerox	Workcentre 6515	-	All	All	All
Operating System	Xerox	Workcentre 6515 Firmware	All	All	All	All

References

Reference	Source	Link
securitydocs.business.xerox.com/wp-content/uploads/2021/03/cert_Security_Mini_Bulletin_XRX21D...	CONFIRM	securitydocs.business.x

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