



CVE-2021-45967

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

CVE	CVE-2021-45967
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-03-18 05:15:00 UTC
Updated	2024-01-03 18:55:00 UTC
Description	An issue was discovered in Pascom Cloud Phone System before 7.20.x. A configuration error between NGINX and a backe

Risk And Classification

Problem Types: CWE-22

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Igniterealtime	Openfire	All	All	All	All
Application	Igniterealtime	Openfire	4.5.0	-	All	All
Application	Pascom	Cloud Phone System	All	All	All	All
Application	Pascom Cloud Phone System	*	All	All	All	All

References

Reference	Source	Link	Tags
The Story of 3 bugs that lead to Unauthorized RCE - Pascom Systems - Tutorial Boy	MISC	tutorialboy24.blogspot.com	
Support & Release Notes	MISC	www.pascom.net	
pascom Server 19	MISC	www.pascom.net	
Pascom: The story of 3 bugs that lead to unauthed RCE. - Blog - Kerbit	MISC	kerbit.io	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, a

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](#).

Free CVE JSON API [cve.report/api](#)

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