



CVE-2021-42638

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

Summary

CVE	CVE-2021-42638
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-02-01 23:15:00 UTC
Updated	2022-02-02 19:14:00 UTC
Description	PrinterLogic Web Stack versions 19.1.1.13 SP9 and below do not sanitize user input resulting in pre-auth remote code execution

Risk And Classification

Problem Types: CWE-77

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Apple	Macos	-	All	All	All
Operating System	Linux	Linux Kernel	-	All	All	All
Application	Printerlogic	Web Stack	All	All	All	All
Application	Printerlogic	Web Stack	19.1.1.13	-	All	All
Application	Printerlogic	Web Stack	19.1.1.13	sp2	All	All
Application	Printerlogic	Web Stack	19.1.1.13	sp3-3	All	All
Application	Printerlogic	Web Stack	19.1.1.13	sp9	All	All

References

Reference	Source	Link	T
PrinterLogic ??? Fixes Critical Vulnerabilities in its suite - TheCyberThrone	MISC	thecyberthrone.in	
Security Bulletin Printerlogic	CONFIRM	www.printerlogic.com	
PrinterLogic vendor addresses triple RCE threat against all connected endpoints The Daily Swig	MISC	portswigger.net	
Paranoids' Vulnerability Research: PrinterLogic Issues Security Alert Paranoids Blog Yahoo Inc.	MISC	www.yahooinc.com	
PrinterLogic fixes high severity flaws in Printer Management SuiteSecurity Affairs	MISC	securityaffairs.co	
PrinterLogic Patches Code Execution Flaws in Printer Management Suite SecurityWeek.Com	MISC	www.securityweek.com	
Eliminate Print Servers PrinterLogic	MISC	printerlogic.com	

CVE Program record	CVE.ORG	www.cve.org	c
NVD vulnerability detail	NVD	nvd.nist.gov	c

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