



CVE-2021-22908

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

Summary

CVE	CVE-2021-22908
State	PUBLIC
Assigner	support@hackerone.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-05-27 12:15:00 UTC
Updated	2024-01-13 18:36:00 UTC
Description	A buffer overflow vulnerability exists in Windows File Resource Profiles in 9.X allows a remote authenticated user with privi

Risk And Classification

Problem Types: CWE-120

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Ivanti	Connect Secure	9.0	-	All	All
Application	Ivanti	Connect Secure	9.0	r1	All	All
Application	Ivanti	Connect Secure	9.0	r2	All	All
Application	Ivanti	Connect Secure	9.0	r2.1	All	All
Application	Ivanti	Connect Secure	9.0	r3	All	All
Application	Ivanti	Connect Secure	9.0	r3.1	All	All
Application	Ivanti	Connect Secure	9.0	r3.2	All	All
Application	Ivanti	Connect Secure	9.0	r3.3	All	All
Application	Ivanti	Connect Secure	9.0	r3.5	All	All
Application	Ivanti	Connect Secure	9.0	r4	All	All
Application	Ivanti	Connect Secure	9.0	r4.1	All	All
Application	Ivanti	Connect Secure	9.0	r5.0	All	All
Application	Ivanti	Connect Secure	9.0	r6.0	All	All
Application	Pulsesecure	Pulse Connect Secure	9.0	-	All	All
Application	Pulsesecure	Pulse Connect Secure	9.0	r1	All	All
Application	Pulsesecure	Pulse Connect Secure	9.0	r1.0	All	All
Application	Pulsesecure	Pulse Connect Secure	9.0	r2	All	All

Application	Pulsesecure	Pulse Connect Secure	9.0	r2.0	All	All
Application	Pulsesecure	Pulse Connect Secure	9.0	r2.1	All	All
Application	Pulsesecure	Pulse Connect Secure	9.0	r3	All	All
Application	Pulsesecure	Pulse Connect Secure	9.0	r3.0	All	All
Application	Pulsesecure	Pulse Connect Secure	9.0	r3.1	All	All
Application	Pulsesecure	Pulse Connect Secure	9.0	r3.2	All	All
Application	Pulsesecure	Pulse Connect Secure	9.0	r3.3	All	All
Application	Pulsesecure	Pulse Connect Secure	9.0	r3.5	All	All
Application	Pulsesecure	Pulse Connect Secure	9.0	r4	All	All
Application	Pulsesecure	Pulse Connect Secure	9.0	r4.0	All	All
Application	Pulsesecure	Pulse Connect Secure	9.0	r4.1	All	All
Application	Pulsesecure	Pulse Connect Secure	9.0	r5.0	All	All
Application	Pulsesecure	Pulse Connect Secure	9.0	r6.0	All	All
Application	Pulsesecure	Pulse Connect Secure	9.0rx	All	All	All
Application	Pulsesecure	Pulse Connect Secure	9.1	-	All	All
Application	Pulsesecure	Pulse Connect Secure	9.1	r1	All	All
Application	Pulsesecure	Pulse Connect Secure	9.1	r10.0	All	All
Application	Pulsesecure	Pulse Connect Secure	9.1	r10.2	All	All
Application	Pulsesecure	Pulse Connect Secure	9.1	r11.0	All	All
Application	Pulsesecure	Pulse Connect Secure	9.1	r11.1	All	All
Application	Pulsesecure	Pulse Connect Secure	9.1	r11.3	All	All
Application	Pulsesecure	Pulse Connect Secure	9.1	r11.4	All	All

References

Reference	Source	Link
Public KB - SA44800 - 2021-05: Out-of-Cycle Advisory: Pulse Connect Secure Buffer Overflow Vulnerability	MISC	kb.pulsesecure.net
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[38839](#) Pulse Connect Secure and Pulse Policy Secure Multiple Vulnerabilities (SA44800)

[38841](#) Pulse Connect Secure Buffer Overflow Vulnerability (SA44800)

© [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](#)