CVE-2020-8260

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2020-8260
State	PUBLIC
Assigner	support@hackerone.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-10-28 13:15:00 UTC
Updated	2021-09-21 17:04:00 UTC
Description	A vulnerability in the Pulse Connect Secure < 9.1R9 admin web interface could allow an authenticated attacker to perform a

Risk And Classification

EPSS: 0.758860000 probability, percentile 0.989040000 (date 2026-04-02)

CISA KEV: Listed on 2021-11-03; due 2022-05-03; ransomware use Unknown

Problem Types: CWE-434

CISA Known Exploited Vulnerability

Vendor	Ivanti
Product	Pulse Connect Secure
Name	Ivanti Pulse Connect Secure Code Execution Vulnerability
Required Action	Apply updates per vendor instructions.
Notes	Reference CISA's ED 21-03 (https://www.cisa.gov/news-events/directives/ed-21-03-mitigate-pulse-connect-secure-product-vulnerabilities) for further guidance and requirements. Note: The due date for addressing this vulnerability aligns with the requirements outlined in ED 21-03. https://nvd.nist.gov/vuln/detail/CVE-2020-8260

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Pulsesecure	Pulse Secure Desktop Client	All	All	All	All
Application	Pulsesecure	Pulse Secure Desktop Client	9.1	-	All	All
Application	Pulsesecure	Pulse Secure Desktop Client	9.1	r1	All	All
Application	Pulsesecure	Pulse Secure Desktop Client	9.1	r2	All	All
Application	Pulsesecure	Pulse Secure Desktop Client	9.1	r3	All	All
Application	Pulsesecure	Pulse Secure Desktop Client	9.1	r3.1	All	All

Application	Pulsesecure	Pulse Secure Desktop Client	9.1	r4	All	All
Application	Pulsesecure	Pulse Secure Desktop Client	9.1	r4.1	All	All
Application	Pulsesecure	Pulse Secure Desktop Client	9.1	r4.2	All	All
Application	Pulsesecure	Pulse Secure Desktop Client	9.1	r5	All	All
Application	Pulsesecure	Pulse Secure Desktop Client	9.1	r6	All	All
Application	Pulsesecure	Pulse Secure Desktop Client	9.1	r7	All	All
Application	Pulsesecure	Pulse Secure Desktop Client	9.1	r7.1	All	All
Application	Pulsesecure	Pulse Secure Desktop Client	9.1	r8	All	All
Application	Pulsesecure	Pulse Secure Desktop Client	9.1	r8.2	All	All
Application	Pulsesecure	Pulse Secure Desktop Client	All	All	All	All
Application	Pulsesecure	Pulse Secure Desktop Client	9.1	-	All	All
Application	Pulsesecure	Pulse Secure Desktop Client	9.1	r1	All	All
Application	Pulsesecure	Pulse Secure Desktop Client	9.1	r2	All	All
Application	Pulsesecure	Pulse Secure Desktop Client	9.1	r3	All	All
Application	Pulsesecure	Pulse Secure Desktop Client	9.1	r3.1	All	All
Application	Pulsesecure	Pulse Secure Desktop Client	9.1	r4	All	All
Application	Pulsesecure	Pulse Secure Desktop Client	9.1	r4.1	All	All
Application	Pulsesecure	Pulse Secure Desktop Client	9.1	r4.2	All	All
Application	Pulsesecure	Pulse Secure Desktop Client	9.1	r5	All	All
Application	Pulsesecure	Pulse Secure Desktop Client	9.1	r6	All	All
Application	Pulsesecure	Pulse Secure Desktop Client	9.1	r7	All	All
Application	Pulsesecure	Pulse Secure Desktop Client	9.1	r7.1	All	All
Application	Pulsesecure	Pulse Secure Desktop Client	9.1	r8	All	All
Application	Pulsesecure	Pulse Secure Desktop Client	9.1	r8.2	All	All

References

Reference
Pulse Secure VPN Remote Code Execution ≈ Packet Storm
Public KB - SA44601 - 2020-10: Security Bulletin: Multiple Vulnerabilities Resolved in Pulse Connect Secure / Pulse Policy Secure / Pulse Sec
CVE Program record
NVD vulnerability detail
CISA Known Exploited Vulnerabilities catalog

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.