CVE-2020-13162

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2020-13162
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-06-16 20:15:00 UTC
Updated	2023-03-01 16:02:00 UTC
Description	A time-of-check time-of-use vulnerability in PulseSecureService.exe in Pulse Secure Client versions prior to 9.1.6 down to 5

Risk And Classification

Problem Types: CWE-367

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Pulsesecure	Pulse Secure Desktop Client	5.3	r1.0	All	All
Application	Pulsesecure	Pulse Secure Desktop Client	5.3	r1.1	All	All
Application	Pulsesecure	Pulse Secure Desktop Client	5.3	r2.0	All	All
Application	Pulsesecure	Pulse Secure Desktop Client	5.3	r3.0	All	All
Application	Pulsesecure	Pulse Secure Desktop Client	5.3	r4.1	All	All
Application	Pulsesecure	Pulse Secure Desktop Client	5.3	r4.2	All	All
Application	Pulsesecure	Pulse Secure Desktop Client	5.3	r5.0	All	All
Application	Pulsesecure	Pulse Secure Desktop Client	5.3	r5.2	All	All
Application	Pulsesecure	Pulse Secure Desktop Client	5.3	r6.0	All	All
Application	Pulsesecure	Pulse Secure Desktop Client	5.3	r7.0	All	All
Application	Pulsesecure	Pulse Secure Desktop Client	9.0	r1.0	All	All
Application	Pulsesecure	Pulse Secure Desktop Client	9.0	r2	All	All
Application	Pulsesecure	Pulse Secure Desktop Client	9.0	r2.1	All	All
Application	Pulsesecure	Pulse Secure Desktop Client	9.0	r3	All	All
Application	Pulsesecure	Pulse Secure Desktop Client	9.0	r3.2	All	All
Application	Pulsesecure	Pulse Secure Desktop Client	9.0	r4	All	All
Application	Pulsesecure	Pulse Secure Desktop Client	9.0	r4.0	All	All

Application	Pulsesecure	Pulse Secure Desktop Client	9.0	r5.0	All	All
Application	Pulsesecure	Pulse Secure Desktop Client	9.0	r6.0	All	All
Application	Pulsesecure	Pulse Secure Desktop Client	9.1	r1.0	All	All
Application	Pulsesecure	Pulse Secure Desktop Client	9.1	r2.0	All	All
Application	Pulsesecure	Pulse Secure Desktop Client	9.1	r3.0	All	All
Application	Pulsesecure	Pulse Secure Desktop Client	9.1	r3.1	All	All
Application	Pulsesecure	Pulse Secure Desktop Client	9.1	r4.0	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	r5.0	All	All
Application	Pulsesecure	Pulse Secure Desktop Client	9.1	r6.0	All	All
Application	Pulsesecure	Pulse Secure Desktop Client	9.1	r7.0	All	All
Application	Pulsesecure	Pulse Secure Desktop Client	5.3	r1.0	All	All
Application	Pulsesecure	Pulse Secure Desktop Client	5.3	r1.1	All	All
Application	Pulsesecure	Pulse Secure Desktop Client	5.3	r2.0	All	All
Application	Pulsesecure	Pulse Secure Desktop Client	5.3	r3.0	All	All
Application	Pulsesecure	Pulse Secure Desktop Client	5.3	r4.1	All	All
Application	Pulsesecure	Pulse Secure Desktop Client	5.3	r4.2	All	All
Application	Pulsesecure	Pulse Secure Desktop Client	5.3	r5.0	All	All
Application	Pulsesecure	Pulse Secure Desktop Client	5.3	r5.2	All	All
Application	Pulsesecure	Pulse Secure Desktop Client	5.3	r6.0	All	All
Application	Pulsesecure	Pulse Secure Desktop Client	5.3	r7.0	All	All
Application	Pulsesecure	Pulse Secure Desktop Client	9.0	r1.0	All	All
Application	Pulsesecure	Pulse Secure Desktop Client	9.0	r2	All	All
Application	Pulsesecure	Pulse Secure Desktop Client	9.0	r2.1	All	All
Application	Pulsesecure	Pulse Secure Desktop Client	9.0	r3	All	All
Application	Pulsesecure	Pulse Secure Desktop Client	9.0	r3.2	All	All
Application	Pulsesecure	Pulse Secure Desktop Client	9.0	r4	All	All
Application	Pulsesecure	Pulse Secure Desktop Client	9.0	r4.0	All	All
Application	Pulsesecure	Pulse Secure Desktop Client	9.0	r5.0	All	All
Application	Pulsesecure	Pulse Secure Desktop Client	9.0	r6.0	All	All
Application	Pulsesecure	Pulse Secure Desktop Client	9.1	r1.0	All	All
Application	Pulsesecure	Pulse Secure Desktop Client	9.1	r2.0	All	All
Application	Pulsesecure	Pulse Secure Desktop Client	9.1	r3.0	All	All
Application	Pulsesecure	Pulse Secure Desktop Client	9.1	r3.1	All	All

Application	Pulsesecure	Pulse Secure Desktop Client	9.1	r4.0	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	r5.0	All	All
Application	Pulsesecure	Pulse Secure Desktop Client	9.1	r6.0	All	All
Application	Pulsesecure	Pulse Secure Desktop Client	9.1	r7.0	All	All
Application	Pulsesecure	Pulse Secure Installer Service	8.3	All	All	All
Application	Pulsesecure	Pulse Secure Installer Service	9.1	All	All	All
Application	Pulsesecure	Pulse Secure Installer Service	9.1	r5.0	All	All
Application	Pulsesecure	Pulse Secure Installer Service	8.3	All	All	All
Application	Pulsesecure	Pulse Secure Installer Service	9.1	All	All	All
Application	Pulsesecure	Pulse Secure Installer Service	9.1	r5.0	All	All

References

Reference
Public KB - SA44503 - 2020-06: Out-of-Cycle Advisory: Pulse Secure Client TOCTOU Privilege Escalation Vulnerability (CVE-2020-13162)
sepcali na Twitterze: "I will share the technical details and a working exploit on https://t.co/oNr2ig1iNs when a patch from the vendor will be av
Pulse Secure Client for Windows <9.1.6 TOCTOU Privilege Escalation (CVE-2020-13162) - Red Timmy Security
Pulse Secure Windows Client Privilege Escalation ≈ Packet Storm
Public KB - Home
Pulse Secure Client For Windows Local Privilege Escalation ≈ Packet Storm
Full Disclosure: Pulse Secure Windows Client <9.1.6 (CVE-2020-13162) - exploit
gsepcali on Twitter: "CVE-2020-13162 is a privilege escalation bug affecting every version of #PulseSecure Client for Windows <9.1R6. I have
sepcali on Twitter: "I will share the technical details and a working exploit on https://t.co/oNr2ig1iNs when a patch from the vendor will be avail
Full Disclosure: Pulse Secure Client < 9.1R6 TOCTOU Privilege Escalation (CVE-2020-13162)
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

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

site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registred 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