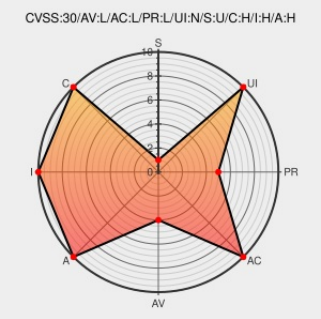
CVE-2018-11479

Published on: 05/25/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:17 PM UTC

CVE-2018-11479

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Windscribe from Windscribe contain the following vulnerability:

The VPN component in Windscribe 1.81 uses the OpenVPN client for connections. Also, it creates a WindScribeService.exe system process that establishes a \\.\pipe\WindscribeService named pipe endpoint that allows the Windscribe VPN process to connect and execute an OpenVPN process or other processes (like taskkill, etc.). There is no validation of the program name before constructing the lpCommandLine argument for a CreateProcess call. An attacker can run any malicious process with SYSTEM privileges through this named pipe.

CVE-2018-11479 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7.8 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	LOW	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: 7.2 - HIGH

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link

Windscribe WindscribeService Named Pipe Privilege Escalation ≈ Packet Storm	packetstormsecurity.com text/html	MISC packetstormsecurity.com/files/156222/Windscribe-WindscribeService-Named-Pipe-Privilege-Escalation.html
vmcs: WindScribe VPN Privilege Escalation	Third Party Advisory sqlulz.blogspot.com text/html	MISC sqlulz.blogspot.com/2018/05/windscribe-vpn-privilege-escalation.html

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Windscribe	Windscribe	1.81	All	All	All
Application	Windscribe	Windscribe	1.81	All	All	All

cpe:2.3:a:windscribe:windscribe:1.81:*:*:*:*:*:*:*:

cpe:2.3:a:windscribe:windscribe:1.81:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→