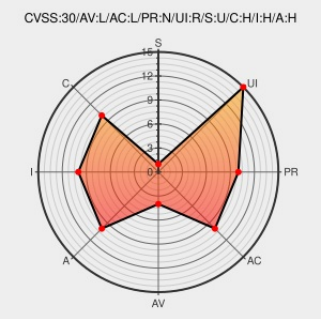
CVE-2018-7484

Published on: 02/25/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:38 PM UTC

CVE-2018-7484

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



Certain versions of Purevpn from Purevpn contain the following vulnerability:

An issue was discovered in PureVPN through 5.19.4.0 on Windows. The client installation grants the Everyone group Full Control permission to the installation directory. In addition, the PureVPNService.exe service, which runs under NT Authority\SYSTEM privileges, tries to load several dynamic-link libraries using relative paths instead of the absolute path. When not using a fully qualified path, the application will first try to load the library from the directory from which the application is started. As the residing directory of PureVPNService.exe is writable to all users, this makes the application susceptible to privilege escalation through DLL hijacking.

CVE-2018-7484 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	NONE	REQUIRED
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: 9.3 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
	Third Party Advisory www.defensecode.com application/pdf	MISC www.defensecode.com/advisories/DC-2018-02-001-PureVPN-Windows-Privilege-Escalation.pdf
SecurityFocus	Third Party Advisory VDB Entry web.archive.org text/html Inactive Link Not Archived	MISC www.securityfocus.com/archive/1/541803

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Purevpn	Purevpn	5.19.4.0	All	All	All
Application	Purevpn	Purevpn	5.19.4.0	All	All	All

cpe:2.3:a:purevpn:purevpn:5.19.4.0:*:*:*:*:windows:*:*:

cpe:2.3:a:purevpn:purevpn:5.19.4.0:*:*:*:*:windows:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→