



CVE-2018-10900

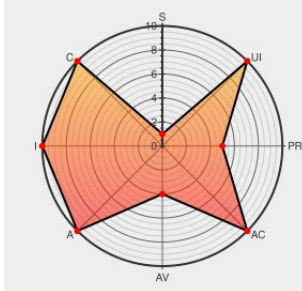
Published on: 07/26/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:22 PM UTC

CVE-2018-10900

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

CVSS:31/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H



Certain versions of [Debian Linux](#) from [Debian](#) contain the following vulnerability:

Network Manager VPNC plugin (aka networkmanager-vpnc) before version 1.2.6 is vulnerable to a privilege escalation attack. A new line character can be used to inject a Password helper parameter into the configuration data passed to VPNC, allowing an attacker to execute arbitrary commands as root.

CVE-2018-10900 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: [UNKNOWN] - networkmanager-vpnc version NetworkManager-vpnc 1.2.6

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
NetworkManager VPNC plugin: Privilege escalation (GLSA	Third Party Advisory	GENTOO GLSA-201808-03

201808-03) — Gentoo security	security.gentoo.org text/html	
Debian -- Security Information -- DSA-4253-1 network-manager-vpnc	Third Party Advisory www.debian.org Deprecated Link text/html	 DEBIAN DSA-4253
service: disallow newlinies in configuration values (CVE-2018-10900) (07ac18a3) · Commits · GNOME / NetworkManager-vpnc · GitLab	Patch Third Party Advisory Vendor Advisory gitlab.gnome.org text/html	 CONFIRM gitlab.gnome.org/GNOME/NetworkManager-vpnc/commit/07ac18a32b4
Network Manager VPNC 1.2.6 - 'Username' Local Privilege Escalation (Metasploit) - Linux local Exploit	Exploit Third Party Advisory VDB Entry www.exploit-db.com Proof of Concept text/html	 EXPLOIT-DB 45313
Bug 1101147 – VUL-0: CVE-2018-10900: NetworkManager-vpnc: local privilege escalation	Exploit Issue Tracking Third Party Advisory bugzilla.novell.com text/html	 CONFIRM bugzilla.novell.com/show_bug.cgi?id=1101147
[SECURITY] [DLA 1454-1] network-manager-vpnc security update	Third Party Advisory lists.debian.org text/html	 MLIST [debian-lts-announce] 20180731 [SECURITY] [DLA 1454-1] network-manager-vpnc security update
Network Manager VPNC - Privilege Escalation (CVE-2018-10900)	Exploit Third Party Advisory pulsesecurity.co.nz text/html	 MISC pulsesecurity.co.nz/advisories/NM-VPNC-Privesc
1605919 – (CVE-2018-10900) CVE-2018-10900 NetworkManager-vpnc: privilege escalation allows to execute arbitrary commands as root	Issue Tracking Patch Third Party Advisory bugzilla.redhat.com text/html	 CONFIRM bugzilla.redhat.com/show_bug.cgi?id=CVE-2018-10900
	Third Party Advisory Vendor Advisory download.gnome.org text/plain	 CONFIRM download.gnome.org/sources/NetworkManager-vpnc/1.2/NetworkManager-vpnc-1.2.6.news

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.

Related QID Numbers

[710253](#) Gentoo Linux NetworkManager Virtual Private NetworkC plugin Privilege escalation Vulnerability (GLSA 201808-03)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating	Debian	Debian Linux	9.0	All	All	All

System						
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Application	Gnome	Network Manager Vpnc	All	All	All	All
Application	Gnome	Network Manager Vpnc	All	All	All	All
cpe:2.3:o:debian:debian_linux:8.0:*****:						
cpe:2.3:o:debian:debian_linux:9.0:*****:						
cpe:2.3:o:debian:debian_linux:8.0:*****:						
cpe:2.3:o:debian:debian_linux:9.0:*****:						
cpe:2.3:a:gnome:network_manager_vpnc:*****:						
cpe:2.3:a:gnome:network_manager_vpnc:*****:						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID→](#)