2019/07/09: SE201901: SoftEther VPN Server NDIS 5.x Windows Local Bridge Driver Local Privilege Escalation Vulnerability

Published: 2019/07/09

Related: CVE-2019-11868

SoftEther VPN Security Advisory articles are published for high impact vulnerabilities (an arbitrary code execution or equivalent).

Summary

A vulnerability in the NDIS 5.x based Local Bridge module for SoftEther VPN 4.29 Build 9680 or older could allow the local Windows-logged-on attacker (who is already logged on to the same computer which run VPN servers) to realize a Windows local authenticated privilege escalation attacks or could result in BSODs.

To exploit this vulnerability, an attacker must log on to the local Windows system which is the same computer which running the SoftEther VPN Server. An attacker could then run a specially crafted program that could exploit the vulnerability.

This vulnerability affects only when the server computer is running the Local Bridge function or the SecureNAT function on Windows 2000, Windows XP, Windows Vista, Windows 7 and Windows 8.0 (not Windows 8.1). Same Windows Server family of these Windows versions could also be affected.

Any systems with Windows 8.1 or Windows 10 (includes Windows Server 2012 R2, 2016, 2019), or Linux, FreeBSD, macOS or Solaris are not to be affected.

This vulnerability affects only when:

1. A VPN system administrator shares a single Windows computer between the VPN server feature and local or remote login terminals for unprivileged users. (e.g. Terminal Service for the organization)
   or
2. A VPN system administrator allows attackers to execute any untrusted arbitrary programs in the local VPN server computer.

Affected Software

- SoftEther VPN Server 4.29 Build 9680 or older for Windows
- SoftEther VPN Bridge 4.29 Build 9680 or older for Windows
- VPN Gate Relay Service 4.29 Build 9680 or older for Windows

VPN servers which run the Local Bridge function in Windows 2000, Windows XP, Windows Vista, Windows 7 and Windows 8.0 (not Windows 8.1) could be affected. Same Windows Server family of these Windows versions could also be affected.

Any systems with Windows 8.1 or Windows 10 (includes Windows Server 2012 R2, 2016, 2019), or Linux, FreeBSD, macOS or Solaris are not to be affected.

Workarounds

- Do not share a single Windows computer between the VPN Server feature and remote login servers for unprivileged users. (e.g. Terminal Service for the organization)

- Do not allow attackers to execute any untrusted arbitrary programs in the local VPN server computer.

Fixed Software

The following software are released to fix this vulnerability.

- SoftEther VPN Server 4.30 Build 9696 Beta (2019/07/08)
- SoftEther VPN Bridge 4.30 Build 9696 Beta (2019/07/08)
- VPN Gate Relay Service 4.30 Build 9696 Beta (2019/07/08)

Note 1) Reboot the Windows after the upgrade installation of SoftEther VPN Server / Bridge if the Local Bridge function is already running on the system since the upgrade installation of SoftEther VPN Server / Bridge will not automatically reload the Local Bridge module until the next reboot of Windows.

Note 2) Version 4.30 is still a beta release. Beta releases are not stable RTM versions. We will release the RTM version after the confirmation of the stability of this beta version

with the adequate period. It is not recommended to install this beta version in the production environment since in the most of production VPN servers, which already observe the above "Workarounds", this vulnerability doesn't affect.

Note 3) 64-bit Windows Vista lack of SHA-2 code signature verification ability while the Version 4.30's Local Bridge driver is digitally signed by the SHA-2 certificate while only commercial SHA-2 code signing certificate is available in the present day. If the Windows Vista systems deny to load the SHA-2 signed modules, disable the kernel mode driver signature check for Windows Vista on the F8 boot menu. This problem is of Windows Vista 64-bit versions. Since the Microsoft's support period of Windows Vista already ended, Microsoft doesn't seems to be willing to address this problem.

Acknowledgments

This fix is based on a report by DownWithUp.