

????SoftEther VPN ??????????????????

[PacketiX VPN 4.0 \(?????????????????\)](#) ?????SoftEther VPN 4.0 ??????????????????

[????????????????? \(SoftEther VPN ??????\)](#)

[????????????????? \(PacketiX VPN ???\)](#)

[?????????????](#)

???: Beta ???RTM ??????????????????????????

- **?????????: SoftEther VPN 4.25 Build 9656 RTM (2018/01/15)**

???: PacketiX VPN 4.25 Build 9656 RTM

?????????????????????????????

???????????????????????????????????? (Max Planck Institute for Molecular Genetics) ?????PacketiX VPN ?

???????? SoftEther VPN ???Guido Vranken

????????????

??VPN ?????

????????????????????VPN ????????????????? (???) ?????????????????????

7 ???

??

- Buffer overread in ParseL2TPPacket()
- Memory corruption in IcmpParseResult
- Missing bounds check in ParseUDP() can lead to invalid memory access
- Out-of-bounds read in IPsec_PPP.c (unterminated string buffer)
- Overlapping parameters to memcpy() via StrToIp6()
- PACK ReadValue() crash vulnerability
- Potential use of uninitialized memory via IPToInAddr6()

4 ????????? (?????????????????????) ???

- Memory leak in NnReadDnsRecord
- Memory leak in RadiusLogin()
- Memory leak via ParsePacketIPv4WithDummyMacHeader
- Remote memory leak in OpenVPN server code

????????:

??? X.509 ?????????????????Alternative Subject Name ????? DNS ?????????????????????????????

Windows ???

- **?????????: SoftEther VPN 4.24 Build 9652 Beta (2017/12/21)**

???: PacketiX VPN 4.24 Build 9652 Beta

Build 9647 ??? 9651 ?????????L2TP/IPsec ? Android Oreo ??????????????????????

????????????????DNS ?????????????????????????????

- **?????????: SoftEther VPN 4.24 Build 9651 Beta (2017/10/23)**

???: PacketiX VPN 4.24 Build 9651 Beta

Build 9647 ?????????OpenVPN Server ?????????????????????

- **?????????: SoftEther VPN 4.23 Build 9647 Beta (2017/10/18)**

???: PacketiX VPN 4.23 Build 9647 Beta

OpenSSL ???????? 1.0.2l ?????????

???????? OpenSSL 1.1.x ?????TLS 1.2 ????????????????? DHE-RSA-CHACHA20-POLY1305, ECDHE-RSA-

CHACHA20-POLY1305 ??????(?????????????????OpenSSL 1.1.x ??????????????????)
TrafficServer / TrafficClient ?? (?????) ??????????????RSS ?????? NIC ????? 10Gbps ??????????????
SSL ?????????????????? RC4-MD5 ?? AES128-SHA ?????
TCP MSS Clamp ??
SecureNAT ?????????????? NAT ??????? DHCP ??????????????????????
USB ?????????????? CryptoID ?????????????????????? DLL ??????????API?????????????????
Mac OS X ??????Select ?????????? INFINITE ?????? CPU ??????????????????????
Syslog ?????? RFC3339 ??? StrictSyslogDatetimeFormat ????? ServerConfiguration ?????
UI ??????????????????

- [Using client parameter in function CtConnect](#)
- [Remove blank line at the start from init file \(Debian\)](#)
- [Stop Radius Delay from counting to next resend](#)
- [Add DH groups 2048,3072,4096 to IPsec IKE](#)
- [Add HMAC SHA2-256, HMAC SHA2-384, HMAC SHA2-512 support](#)
- [Openvpn extend ciphers](#)
- [Fixed RSA key bits wrong calculation for certain x509 certificate](#)
- [Added support for RuToken USB key PKCS#11](#)
- [OpenSSL 1.1 Port](#)

• **?????????: SoftEther VPN 4.22 Build 9634 Beta (2016/11/27)**

????: PacketiX VPN 4.22 Build 9634 Beta

TLS 1.2 ??????TLS 1.2 ??????????????AES128-GCM-SHA256?AES128-SHA256?AES256-GCM-SHA384?
AES256-SHA256?DHE-RSA-AES128-GCM-SHA256?DHE-RSA-AES128-SHA256?DHE-RSA-AES256-GCM-
SHA384?DHE-RSA-AES256-SHA256?ECDHE-RSA-AES128-GCM-SHA256?ECDHE-RSA-AES128-SHA256?
ECDHE-RSA-AES256-GCM-SHA384???ECDHE-RSA-AES256-SHA384 ??????
??? TLS ?????????? / ??????????????????????????????VPN Server ?????????? Tls_Disable1_0?Tls_Disable1_1 ???
Tls_Disable1_2 ?????????????????????? TLS ??????????????????????
OpenVPN ? TLS 1.2 ?????????????????????????????????????
OpenSSL ????????? 1.0.2j ?????????????????
Windows Server 2016 ??????????
2038 ?????????????????
????????? HTTPS ?????????????????? SNI ??????????????????????
RADIUS ?????????????? "Called-Station-ID (30)" ?????????? ?? HUB ??????????????????????????????????
????? 3 ??????????????????ARP ?????????? 1 ??????
Windows 10 ? VPN Server ??????????????????????
????????????????? RSA ????????? 4096 bit ?????????????
USB ??????CryptoID?????????????????
????? UI ??????????????????????

- [Fix that ParseTcpOption doesn't work correctly](#)
- [Add LSB header](#)
- [Support Debian package build on aarch64 architecture](#)
- [Support Debian package build on ARMv7l architecture](#)
- [cppcheck issues](#)
- [Default to TLS connections only](#)
- [Allow specific SSL/TLS versions to be disabled](#)
- [Adding Radius AVP Called-Station-Id](#)
- [Fixed typo](#)
- [Update CentOS makefiles and spec file](#)
- [Systemd service configuration files for SoftEther](#)
- [Fix set initialization, set.OnlyCapsuleModeIsInvalid could be garbage](#)

??????????2013 ? 10 ?? Microsoft ???????????? Windows 8.1 ??? Windows Server 2012 R2 (RTM ?) ??
??
??
??
??

• **????: SoftEther VPN 1.01 Build 9379 RTM (2013/08/18)**

????: PacketiX VPN 4.01 Build 9379 RTM

??

??PacketiX VPN 4.0 / SoftEther VPN 1.0 ???
??

PacketiX VPN 4.0 ??? SoftEther VPN 1.0 (Server ??? Bridge) ???VPN Server Manager ??? vpcmd ??
??
??
??
??
?? (???) ?????? HUB ?????????? HUB ???
?? HUB ???
??

• **????: PacketiX VPN 4.00 Build 9378 RTM (2013/08/14) * PacketiX VPN ??**

????????? PacketiX VPN ??? 9378 ???

• **????: SoftEther VPN 1.00 Build 9376, 9377 RTM (2013/08/03) * SoftEther VPN ??**

This is a minor fix.
Improvement Stability of NAT Traversal.
Add HTTP User-Agent Indication Behavior when using VPN Gate Client.

• **????: SoftEther VPN 1.00 Build 9371 RTM (2013/07/25)**

????: PacketiX VPN 4.00 Build 9371 RTM

????????? RTM (???) ???
??
SoftEther VPN ?????????????? SoftEther VPN ?????????????????????????????????

• **Ver 1.00 Build 9367 RC4 (2013/06/21)**

?????????RTM (???) ?????????????????????????????????

• **Ver 1.00 Build 9091 RC3 (2013/05/19)**

?????????? RC3 ??????????????RC3 ?????? (GA: Generally Available) ?????????????????
- L2TPv3 ??? EtherIP over IPsec ?????????????? vpcserver ?????????????????????????????
- VPN ?????????????????? vpcmd ?????????? HUB ?????????????????????????????????
- VPN ?????????????????? vpcmd ???
- ?????? DNS ?????? NAT ?????????????????????

• **Ver 1.00 Build 9079 RC2 Fix17 (2013/05/05)**

??

• **Ver 1.00 Build 9078 RC2 Fix16 (2013/04/28)**

?? HUB ?????????? "deny_empty_password" ?????????????????????????????????
??
????????????????

IPv6 DNS ??????????????????

- **Ver 1.00 Build 9074 RC2 Fix15 (2013/04/24)**
?????? DNS ??????????????????
- **Ver 1.00 Build 9071 RC2 Fix14 (2013/04/20)**
?????????????????
- **Ver 1.00 Build 9070 RC2 Fix13 (2013/04/18)**
?? (Win32 ??????)?
??
- **Ver 1.00 Build 9069 RC2 Fix12 (2013/04/17)**
SSL ??????????????????????
TCP ??????????????????????
- **Ver 1.00 Build 9053 RC2 Fix11 (2013/04/08)**
UDP ??????????????????????
?????: IKE ??? OpenVPN (UDP ???) ??????????????????????
- **Ver 1.00 Build 9045 RC2 Fix10 (2013/04/02)**
?????????????????????
- **Ver 1.00 Build 9043 RC2 Fix9 (2013/04/01)**
HTTP ??????????????????????
UDP ??????????????????
?????: SecureNAT ??????????????????????
- **Ver 1.00 Build 9035 RC2 Fix8 (2013/03/26)**
?????????: X.509 ?????????????????????? SSL-VPN ???
??
- **Ver 1.00 Build 9033 RC2 Fix7 (2013/03/22)**
?????????
- **Ver 1.00 Build 9030 RC2 Fix6 (2013/03/21)**
?????: L2TP/SSTP/OpenVPN ??????????????????????
- **Ver 1.00 Build 9029 RC2 Fix5 (2013/03/17)**
?????????????
- **Ver 1.00 Build 9027 RC2 Fix4 (2013/03/12)**
?????????
- **Ver 1.00 Build 9026 RC2 Fix3 (2013/03/10)**
?????: DDNS ??????????????????
- **Ver 1.00 Build 9024 RC2 Fix2 (2013/03/09)**
?????: Windows ? VPN over DNS ??????????

- **Ver 1.00 Build 9023 RC2 Fix1 (2013/03/08)**
?????????
- **Ver 1.00 Build 9022 RC2 (2013/03/08)**
?????????