2023/06/30: SE202301: Security Advisory: CVE-2023-27395 etc: Fixed 6 vulnerabilities of SoftEther VPN in cooperation with Cisco Systems, Inc.

June 30, 2023 by Daiyuu Nobori

Related: CVE-2023-27395, CVE-2023-22325, CVE-2023-32275, CVE-2023-27516, CVE-2023-32634, CVE-2023-31192

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

The SoftEther VPN project received a high level code review and technical assistance from Cisco Systems, Inc. of the United States from April to June 2023 to fix several vulnerabilities in the SoftEther VPN code.

The risk of exploitation of any of the fixed vulnerabilities is low under normal usage and environment, and actual attacks are very difficult. However, SoftEther VPN is now an open source VPN software used by 7.4 million unique users worldwide, and is used daily by many users to defend against the risk of blocking attacks by national censorship firewalls and attempts to eavesdrop on communications. Therefore, as long as the slightest attack possibility exists, there is great value in preventing vulnerabilities as much as possible in anticipation of the most sophisticated cyber attackers in the world, such as malicious ISPs and man-in-the-middle attackers on national Internet communication channels. These fixes are important and useful patches for users who use SoftEther VPN and the Internet for secure communications to prevent advanced attacks that can theoretically be triggered by malicious ISPs and man-in-the-middle attackers on national Internet communication pathways.

The fixed vulnerabilities are CVE-2023-27395, CVE-2023-22325, CVE-2023-32275, CVE-2023-27516, CVE-2023-32634, and CVE-2023-31192. All of these were discovered in an outstanding code review of SoftEther VPN by Cisco Systems, Inc.

We would like to sincerely acknowledge Cisco Systems, Inc. and Lilith, a security researcher in the Cisco Talos division, for their contributions to improving security for users of SoftEther VPN over the Internet.

SoftEther VPN is open source software (Apache 2.0 license) and all modifications to the source code are publicly available.

The list of vulnerabilities is as follows. Of particular interest are vulnerabilities 1, 2, and 6, which were difficult to find without a thorough code review.

1. CVE-2023-27395: Heap overflow in SoftEther VPN DDNS client functionality at risk of crashing and theoretically arbitrary code execution caused by a malicious man-in-the-middle attacker such like ISP-level or on national Internet communication channels

2. CVE-2023-22325: Integer overflow in the SoftEther VPN DDNS client functionality could result in crashing caused by a malicious man-in-the-middle attacker such like ISP-level or on national Internet communication channels

3. CVE-2023-32275: Vulnerability that allows the administrator himself of a 32-bit version of VPN Client or VPN Server to see the 32-bit value heap address of each of trusted CA's certificates in the VPN process

4. CVE-2023-27516: If the user forget to set the administrator password of SoftEther VPN Client and enable remote administration with blank password, the administrator password of VPN Client can be changed remotely or VPN client can be used remotely by anonymouse third person

5. CVE-2023-32634: If an attacker succeeds in launching a TCP relay program on the same port as the VPN Client on a local computer running the SoftEther VPN Client before the VPN Client process is launched, the TCP relay program can conduct a man-in-the-middle attack on communication between the administrator and the VPN Client process

6. CVE-2023-31192: When SoftEther VPN Client connects to an untrusted VPN Server, an invalid redirection response for the clustering (load balancing) feature causes 20 bytes of uninitialized stack space to be read

The details are explained below.

1. CVE-2023-27395: Heap overflow in SoftEther VPN DDNS client functionality at risk of crashing and theoretically arbitrary code execution caused by a malicious man-in-the-middle attacker such like ISP-level or on national Internet communication channels

(1) Severity

CVSS v3.1: AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H (8.1)
However, as noted below, the attack requires a man-in-the-middle attack on the TCP communication between the Dynamic DNS (DDNS) client function and the DDNS server. Even in that case, arbitrary code execution has not been demonstrated, only a theoretical possibility exists. Nevertheless, we recommend updating the software as a precautionary measure.

(2) Overview

In the Dynamic DNS (DDNS) client function built into SoftEther VPN Server / Bridge (the same below), an attacker who succeeds in a man-in-the-middle attack on the TCP communication between the VPN Server and the DDNS server can generate a heap overflow and cause the VPN Server program to stop. The attacker must control the communication path between the VPN Server and the Internet to be able to conduct a man-in-the-middle attack. Because of the heap overflow, although usually prevented by heap address randomization and heap corruption detection possessed by the OS and runtime, the theoretical possibility exists that it can be exploited for arbitrary code execution. Therefore, an update of the VPN Server is recommended.

(3) Affected versions

SoftEther VPN 4.41 Build 9787 RTM and earlier

(4) Conditions necessary for a successful attack against this vulnerability

The attacker must have control over the Internet connection lines (ISP, WiFi, or other infrastructure) or reference DNS servers to which the VPN server is connected to the Internet, and be in a position to execute a man-in-the-middle attack that rewrites the contents of communications, such as tampering with TCP/IP communications between a dynamic DNS client and a dynamic DNS server or DNS communications preceding this.

(5) Details

SoftEther VPN Server has a dynamic DNS client (DDNS) function. The dynamic DNS client function periodically registers or updates itself with the dynamic DNS server. The dynamic DNS server https://www.softether.net/ issues "****.softether.net" (where *** is an arbitrary string desired by the user).

The communication (RPC, HTTP-based Remote Procedure Call) by the SoftEther VPN Server to register itself with the dynamic DNS server or to update its registration is performed in the background.
If an attacker meets the above "conditions," such as the attacker controlling the communication path such as the ISP line to which the VPN Server is connected to the Internet, the attacker can rewrite the contents of the RPC between the VPN Server and the dynamic DNS server, or can respond with a false RPC.
By altering or forging the RPC response and including abnormal data in the RPC response, the attacker causes a heap space overflow in the SoftEther VPN Server process that receives the response.
If the VPN Server program crashes, all users connected to the VPN Server will be disconnected and VPN communication will be unavailable until the process is restarted. Therefore, an attacker who meets the above conditions can realize a DoS attack that disconnects VPN communication.
Note that this vulnerability is a heap area overflow, which is detected by the heap area corruption checks possessed by the OS and C runtime and causes the program to crash, but in principle, the possibility that arbitrary code execution is possible cannot be denied if an elaborate attack communication packet is created. However, neither the primary discoverer nor the developers have so far succeeded in demonstrating that arbitrary code execution is possible.
In addition to identifying and fixing the area where the heap overflow occurs, this vulnerability patch provides double prevention by changing the communication between the DNS client function and the DDNS server function, which previously used HTTP, to SSL.

2. CVE-2023-22325: Integer overflow in the SoftEther VPN DDNS client functionality could result in crashing caused by a malicious man-in-the-middle attacker such like ISP-level or on national Internet communication channels

(1) Severity

CVSS v3.1: AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H (5.9)

(2) Overview

In the dynamic DNS (DDNS) client function built into SoftEther VPN Server, an attacker who succeeds in a man-in-the-middle attack on the TCP communication between the VPN Server and the DDNS server can cause an integer overflow and stop only the DDNS client function part of the VPN Server program. If the DDNS client portion of the VPN Server program is stopped, even if the server's IP address changes, the change cannot be registered with the DDNS server until the VPN Server program is restarted. Then this causes a practical problem. An attacker needs to control the communication path between the VPN Server and the Internet to be able to conduct a man-in-the-middle attack.

(3) Affected versions

SoftEther VPN 4.41 Build 9787 RTM and earlier

(4) Conditions necessary for a successful attack against this vulnerability

The attacker must have control over the Internet connection lines (ISP, WiFi, or other infrastructure) or reference DNS servers to which the VPN server is connected to the Internet, and be in a position to execute a man-in-the-middle attack that rewrites the contents of communications, such as tampering with TCP/IP communications between a dynamic DNS client and a dynamic DNS server or DNS communications preceding this.

(5) Details

This vulnerability is similar to CVE-2023-27395. The attacker needs to send a specially crafted packet to the VPN Server to increase the maximum size of the receive buffer before tampering with the DDNS RPC response. That in itself does not cause a problem, but if the communication with the DDNS server is subsequently tampered with or the DDNS server is replaced by a false server, and the DDNS server responds with a value stating a certain large data size, the DDNS client will attempt to allocate memory space for that large data size. The DDNS client attempts to allocate memory space for that large data size. Here, an overflow on an integer variable occurs, causing a simple infinite loop and code stoppage in some DDNS client functions.
In this vulnerability patch, the part where the integer overflow occurs has been identified and fixed, and the communication between the DNS client function and the DDNS server function, which previously used HTTP, has been converted to SSL to provide a double layer of prevention.

3. CVE-2023-32275: Vulnerability that allows the administrator himself of a 32-bit version of VPN Client or VPN Server to see the 32-bit value heap address of each of trusted CA's certificates in the VPN process

(1) Severity

5.5 - CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N

(2) Overview

SoftEther VPN Client and SoftEther VPN Server have a function to manage the list of trusted certificate authorities (CA). The first address of the heap address that holds the certificate is responded. This is because the heap address is used as a unique ID in the memory of the certificate. This means that the administrator himself can infer the heap state from outside the VPN process without dumping the process.
Whether or not this is really a vulnerability (i.e., whether or not it is an infringement of confidentiality for the administrator who manages and controls the VPN process to be able to know the heap address of an object in the process) should be discussed, but it is true that the heap address of a certificate. The heap address of an object is important only within a single process that manages it, and outputting it outside the process is not normally expected, except for exceptional functions such as debuggers that output internal states, so we decided to fix this issue.
In the 64-bit version of SoftEther VPN, heap address is not used, so heap address is not displayed. The 64-bit version uses a hash value based on the heap address instead. However, according to the opinion of the first discoverer of the vulnerability, it is possible to use the rainbow table of hashes to guess the original heap address.

(3) Affected versions

SoftEther VPN 4.41 Build 9787 RTM and earlier

(4) Conditions necessary for a successful attack against this vulnerability

An attacker who desires to peek at the heap address must have administrative privileges to the target VPN Server or VPN Client and must be authenticated as an administrator.

(5) Details

In this patch, both the 32-bit and 64-bit versions have been improved to make it difficult to even create a rainbow table by using a random random number seed specific to the instance of the process when generating a unique enumeration identifier from the heap address.

4. CVE-2023-27516: If the user forget to set the administrator password of SoftEther VPN Client and enable remote administration with blank password, the administrator password of VPN Client can be changed remotely or VPN client can be used remotely by anonymouse third person

(1) Severity

7.0 - CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:L
However, the problem occurs only when the administrator forgot to set the administrator password of SoftEther VPN Client and also enable remote administration.

(2) Overview

SoftEther VPN Client is divided into two parts: the main VPN Client process and the VPN Client Manager or vpncmd command line utility. The communication between the main process and the VPN Client Manager or vpncmd command line utility is done via TCP-based RPC. Normally, the VPN Client process itself and the VPN Client Manager or vpncmd command line utility reside on the same computer. Therefore, initially, they can only be controlled from the same computer (localhost, 127.0.0.1).
SoftEther VPN Client has a remote administration feature that allows the administrator to change the configuration of the VPN Client process and allow control from a remote computer (other than localhost).
If the administrator has configured the VPN Client to allow remote administration and has forgotten to set the administration password, an attacker with TCP access can connect to the VPN Client without a password, set the password without permission, and use the VPN Client functions freely. It is dangerous.

(3) Affected versions

SoftEther VPN 4.41 Build 9787 RTM and earlier

(4) Conditions necessary for a successful attack against this vulnerability

The administrator of the SoftEther VPN Client must have forgotten to set the administrator password and must have enabled remote administration. Furthermore, the VPN Client must be exposed to the Internet or otherwise able to communicate with the attacker.

(5) Details

This problem does not occur by default because SoftEther VPN Client is a default secure implementation and remote administration is disabled by default. However, it is possible that the administrator may forget to set the password and enable remote administration. Whether this is a vulnerability or not is a matter of debate. However, it can be assumed that a normal administrator would set a password almost 100% of the time when enabling remote management of the VPN Client. If the administrator forgets to set the password, changing the implementation so that the user authentication in remote administration is not allowed to pass has the advantage of improving security, and on the other hand, it has few disadvantages.
Therefore, we have modified the behavior of SoftEther VPN Client to prohibit remote connections if the administrator has forgotten the administrator password setting and has enabled remote administration, thereby improving security.

5. CVE-2023-32634: If an attacker succeeds in launching a TCP relay program on the same port as the VPN Client on a local computer running the SoftEther VPN Client before the VPN Client process is launched, the TCP relay program can conduct a man-in-the-middle attack on communication between the administrator and the VPN Client process

(1) Severity

7.8 - CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

(2) Overview

SoftEther VPN Client is divided into two parts: the main VPN Client process and the VPN Client Manager or vpncmd command line utility. The communication between the main process and the VPN Client Manager or vpncmd command line utility is done via TCP-based RPC. Normally, the VPN Client process itself and the VPN Client Manager or vpncmd command line utility reside on the same computer. Therefore, initially, they can only be controlled from the same computer (localhost, 127.0.0.1).
Assume that an attacker has already infiltrated the local computer on which the VPN Client is running by other means (e.g., knowing the OS's user password) and can freely launch processes on the local machine. In addition, suppose that the attacker succeeds in launching a TCP relay program on the same port as the VPN Client before the VPN Client is launched. In this case, if the VPN Client is launched at a later time, the VPN Client avoids using the conflicting TCP port number and increments the TCP port number in turn, using the first free port it finds. This is referred to here as the DynamicPortListener function. In this case, the attacker's TCP relay program can accept TCP RPC connections from the administrator's VPN Client Manager and relay the communication to the true VPN Client process modified by the DynamicPortListener function. If the administrator has enabled remote administration and has set an administrator password, the TCP relay program can hijack the content of the communication after authentication.

(3) Affected versions

SoftEther VPN 4.41 Build 9787 RTM and earlier

(4) Conditions necessary for a successful attack against this vulnerability

The attacker must be able to infiltrate the computer on which the VPN Client is running by other means beforehand, and must be able to launch arbitrary programs locally.

(5) Details

In order for this attack to be realized, the target computer must already be logged in by the attacker and ready to execute arbitrary programs, and in practice, the threat is small. However, there are environments where UNIX computers are SSH-shared by multiple users. And it is possible that one user may have malicious intent. In such an environment, it is desirable to have some countermeasures against this vulnerability.
In this patch, a function to enable/disable the DynamicPortListener function has been added to the VPN Client. The reason why the DynamicPortListener function is enabled by default in the Windows environment and disabled by default in the UNIX

environment is that when using the VPN Client on Windows, it is usually assumed that one user occupies one terminal.
The DynamicPortListener function can be enabled/disabled by setting the DisableRpcDynamicPortListener setting value to true/false in the vpn_client.config configuration file.

6. CVE-2023-31192: When SoftEther VPN Client connects to an untrusted VPN Server, an invalid redirection response for the clustering (load balancing) feature causes 20 bytes of uninitialized stack space to be read

(1) Severity

5.3 - CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N

(2) Overview

This is a very interesting vulnerability, and the outstanding uniqueness of the first discoverer's point of view on this vulnerability is well expressed.
When the VPN Client (including the Cascade Connection function of VPN Server / Bridge) connects to the VPN Server, if the VPN Server has clustering enabled, after successful user authentication, a redirect response is returned for load balancing and fault tolerance. The redirect response contains a 20-byte one-time token code for the redirect destination called a "Ticket", which is typically copied in memory from the packet from which the VPN Client received the redirect response into a 20-byte UCHAR ticket[20] variable in the C language. If the redirection response packet does not contain a Ticket value, it is not copied. However, in this case, the variable UCHAR ticket[20] is uninitialized, and what it contains is neither defined nor predictable.
The VPN Client then connects to the VPN Server to which it was redirected, and at that time, a copy of the 20-byte UCHAR ticket[20] variable in the C language that was copied earlier is sent to the destination VPN Server as a the VPN Server is then sent a copy of the 20-byte UCHAR ticket[20] variable in the C language that was just copied. Here, the uninitialized 20-byte value is sent. This enables the destination VPN Server to obtain the value of the uninitialized 20-byte variable on the stack.

(3) Affected versions

SoftEther VPN 4.41 Build 9787 RTM and earlier

(4) Conditions necessary for a successful attack against this vulnerability

Prior to the attack, the attacker needs to induce users of the VPN Client to connect toward an unintended VPN Server by using man-in-the-middle attacks on the Internet, DNS rewriting attacks, or other techniques.
In addition, the VPN Client has a function to verify the SSL certificate of the VPN Server; if SSL certificate verification is enabled, the attacker needs to steal the private key of the SSL certificate by some means, and then launch a fake VPN Server.

(5) Details

This vulnerability allows a malicious VPN Server to obtain the contents of a 20-byte variable called UCHAR ticket[20] that has not been initialized when a VPN Client connects.
The question is what is in the uninitialized UCHAR ticket[20]. The contents of an uninitialized variable is undefined and unpredictable. In most cases, when the stack depth of another function called earlier is sufficient, the values of variables written in memory areas that happen to exist at the same stack depth in that other function (e.g., integer values of int i, j, k, etc. in a for loop) remain intact and are read back. This is not particularly useful information for an attacker. However, theoretically, there is a possibility that a fragment of confidential information (e.g. authentication information, heap memory address, etc.) could accidentally overlap with the 20-byte area. In this case, the attacker can read out significant information for his attack. Note that unlike higher-level languages, C language variables contain little or no meta-information (management information for managed variables) that encompasses the variable domain, so even if an attacker obtains a 20-byte value, the meaning of the contents is almost always unknown by the attacker, and the possibility of it being useful is small. Nevertheless, if there is even a small theoretical possibility that the contents of an uninitialized variable are externally exposed that could be exploited, it is important to zero-clear this as a precautionary measure to increase security as much as possible.

New build with fixes for the above vulnerabilities

A new build was released on June 30, 2023.

- **VPN 4.42 Build 9798 RTM or later**