

FACTSHEET FS-2009-04

'TCP sockstress': Several vulnerabilities in the implementation of TCP

On 8 September 2009 a number of software and hardware vendors released a patch for a series of vulnerabilities caused by implementation errors in one of the foundations of the internet¹: the Transmission Control Protocol or TCP for short. This protocol is one of the fundamental protocols for communication over networks, and therefore also the internet. A large range of TCP implementations appear to be vulnerable. These vulnerabilities were already discovered in October 2008, but given the nature and extent of the problem, it was necessary to give suppliers the time to check their implementations. It is expected that many suppliers will issue patches in the near future to remedy such vulnerabilities in the TCP protocol.

This factsheet lists the known facts regarding these vulnerabilities and provides recommendations that can help to reduce the abuse of such vulnerabilities or to limit their impact.

What is going on?

In October 2008 the researchers Jack Louis and Robert Lee of the Outpost24 company announced that they had discovered various vulnerabilities in different TCP implementations. These implementation errors allow an attacker to carry out a Denial of Service attack. What is new is that this attack can be performed with very few resources and barely any network bandwidth, unlike most (D)DoS attacks² known at the present time. No details have been announced yet and there is hefty speculation on whether this is really a (new) problem. Given that TCP is used by a huge variety of applications, the consequences will be partly determined by the nature of the application. Because of the potentially serious impact it was decided to ensure that the patch process was coordinated as much as possible. CERT-FI³ is taking the lead here and provides a list of suppliers who have patches available in its advisory. This advisory can be found on: <https://www.cert.fi/haavoittuvuudet/2008/tcp-vulnerabilities.html>

In November 2008 the researchers demonstrated the attack to the staff at GOVCERT.NL and it was confirmed that the problem is both real and new.

An overview of the most important

- > There are implementation errors in numerous TCP implementations. TCP is one of the basic protocols for network communication.
- > Detailed information is not public at this moment.
- > At this time no exploit code is publicly available, but this can be expected in the short term as patches become available.
- > Abuse of the exploit code could make it relatively easy to launch a Denial of Service attack without having to make too much of an effort. The result would be the failure of communication and/or web services.
- > Various suppliers have issued updates to cure the vulnerability in their TCP implementation.
- > Checking vulnerable implementations and if need be patching are the main actions that organizations can take to limit the risks.

¹You can read more about different vulnerabilities in the foundations of the internet in the GOVCERT.NL Trend Report 2009, to be found at www.govcert.nl

²You can read more about (D)DOS attacks in the Govcert white paper 'Attack as defence against DOS attacks'. You can download this white paper from <http://www.govcert.nl/render.html?it=50>. This white paper gives more information about DOS attacks but does not take into account the technology described in this factsheet!

³ CERT-FI is the national CERT (Computer Emergency Response Team) in Finland.

'Vulnerabilities'

The internet uses the TCP/IP protocol to exchange data between systems and applications. To set up a connection between for example a client and a server, TCP uses a 'three-way-handshake'. The 'TCP sockstress' research showed that the system sources for the purposes of a TCP session initiated via a 'three way handshake' could be misused. These system sources include counters, timers and available memory at kernel level. With a variety of attacks, such as various 'window sizes', it is possible to permanently reserve available resources. By means of a trick, the attacker can administer these connections in such a way that this costs the attacker almost no resources. The result is that an application, or even the operating system, becomes unstable and inaccessible. This means that an application or system becomes permanently or temporarily inaccessible. Permanent problems at the application level can be solved by a restart of the application. For a permanent problem at the operating system level it is necessary to restart the entire system. The impact as regards exploiting vulnerabilities varies depending on the application and the platform.

It is difficult to detect the attack due to the limited bandwidth that is required, most of all because the network traffic resembles ordinary legitimate network traffic. An attacker can therefore cause serious problems for servers with minimal computing power and bandwidth (e.g. web and FTP server) and infra-components (e.g. routers, firewalls and switches).

TCP sockstress attacks are nothing new⁴. What is new is that only very limited resources are required for this version.

What is the impact of the vulnerability?

The general impact when vulnerabilities are exploited is a Denial of Service. The extent of the impact depends on the nature of the application and the operating system which the application uses.

The extent of the impact can be divided into three categories:

1. Temporary impact on the application

The application will temporarily not accept any new connections at the time of the attack. When the attack is terminated, the application returns to a usable state and is therefore accessible again.

2. Permanent impact on the application

The application does not accept any new connections when the attack is launched. The application will then remain in this permanent state, even after the attack has been terminated. A restart of the application will solve the problem.

3. Permanent impact on the operating system

The kernel of the operating system is no longer able to carry out essential tasks after the attack has been launched. The result is that the system becomes completely unusable. Restarting the system is in this case the only solution.

⁴In June 2009 Prack magazine described a different method for carrying out a DOS attack on TCP (<http://www.phrack.com/issues.html?issue=66&id=9#article>). This article describes not precisely the same but rather a similar problem.

What can you do about this?

The question is what actions your organization needs to perform to reduce the risk of misuse of this vulnerability. Below is a list of the most significant actions you can consider:

1. Step one is to make an inventory of whether your organization is using a vulnerable TCP implementation. Unfortunately only a small number of suppliers have made it known at the present time whether their products are vulnerable, and if applicable, whether patches have been made available. At the moment many suppliers are investigating whether their products are vulnerable. The possible vulnerabilities can therefore range over a wide variety of applications and operating systems. CERT-FI maintains a list of suppliers, to be found at <https://www.cert.fi/haavoittuvuudet/2008/tcp-vulnerabilities.html>
US-CERT published an overview of all suppliers informed about this sockstress issue, including a status update for each supplier (unknown, vulnerable, not-vulnerable). See <http://www.kb.cert.org/vuls/id/723308>
2. There are no tools available yet to investigate yourself whether your implementations are vulnerable. Tools have been made available to suppliers.
3. If your TCP implementation appears vulnerable as a result from your inventory, then it is important to patch this as soon as possible. You can use the information from GOVCERT.NL advisory 2009-255⁵ for this.
4. If patching is impossible, then you can see whether the countermeasures as described in the English paper, 'Security assessment of the TCP protocol', are applicable to your organization and situation. You can find this paper on the website of the British Centre for the Protection of National Infrastructure (CPNI) <http://www.cpni.gov.uk/Products/technicalnotes/Feb-09-security-assessment-TCP.aspx>
5. Be on the lookout for security patches issued by your supplier. It is expected that more suppliers will issue patches for these vulnerabilities.

Patches issued in the meanwhile; list of suppliers (as on December 7th 2009):

Various suppliers will issue patches in the near future if their platforms are vulnerable. In its advisory, CERT-FI, our Finnish partner, which coordinates this vulnerability, gives a list of suppliers that have patches available or suppliers who state that they are not vulnerable. This advisory can be found on: <https://www.cert.fi/haavoittuvuudet/2008/tcp-vulnerabilities.html>

The following suppliers have in the meanwhile made updates available. We advise you to install these updates.

Aruba

<https://airheads.arubanetworks.com/article/arubaos-exposure-cert-fi-advisory-outpost24-tcp-issues>

Bluecoat

Certain Bluecoat products are vulnerable. More information is available at the Bluecoat website, (a valid login is necessary)

<https://kb.bluecoat.com/index?page=content&id=SA38>

<https://kb.bluecoat.com/index?page=content&id=SA37>

<https://kb.bluecoat.com/index?page=content&id=SA36>

<https://kb.bluecoat.com/index?page=content&id=SA35>

<https://kb.bluecoat.com/index?page=content&id=SA34>

⁵ GOVCERT.NL advisories are only available to participants.

Checkpoint

https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk42723
https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk42725

Cisco

<http://www.cisco.com/warp/public/707/cisco-sa-20090908-tcp24.shtml>

Microsoft

<http://www.microsoft.com/technet/security/bulletin/MS09-048.msp>

McAfee

Email and web security appliance software is vulnerable.

<https://kc.mcafee.com/corporate/index?page=content&id=KB66963>

Nortel

<http://support.nortel.com/go/main.jsp?cscat=BLTNDetail&id=971633>

Wind River

WindRiver indicated VX Works vulnerable

<https://support.windriver.com/olsPortal/faces/maintenance/downloadDetails.jspx?contentid=020900>
<http://windriver.com/support/>

The following suppliers have stated that their products are vulnerable. However, they have not yet made a patch available.

Juniper

Juniper has confirmed that its equipment is vulnerable. But Juniper considers the described vulnerabilities to be generic, previously published attacks on the TCP protocol. For this reason Juniper recommends to follow up the 'best common practices' which it has previously published. You will find information on this in the following Juniper advisory:

<https://www.juniper.net/alerts/viewalert.jsp?actionBtn=Search&txtAlertNumber=PSN-2008-10-041>

Red Hat

Red Hat has stated that Red Hat Enterprise Linux is vulnerable, but that Red Hat will not issue any updates for this OS. <http://kbase.redhat.com/faq/docs/DOC-18730>

SUSE

SUSE has stated that SUSE Linux is vulnerable, but that SUSE will not issue any updates for this OS.

http://www.novell.com/linux/security/advisories/2009_47_tcpip.html

Sun Microsystems

Sun has confirmed that its equipment is vulnerable. A patch has not yet been made available. You will find more information at <http://sunsolve.sun.com/search/document.do?assetkey=1-66-267088-1>

Stonesoft

Stonesoft has stated that certain versions of their products are vulnerable. A patch has not yet been made available http://www.stonesoft.com/en/support/security_advisories/2009_17_09.html

The following suppliers have stated that they are not vulnerable.

VMWare

VMWare has stated that it is not vulnerable

Clavister

Clavister has stated that it is not vulnerable

Fortinet

Fortinet has stated that it is not vulnerable