

## FACTSHEET FS-2009-04

**'TCP sockstress': Meerdere kwetsbaarheden in de implementatie van TCP**

Op 8 september 2009 brengt een aantal soft- en hardwareleveranciers patches uit voor een serie van kwetsbaarheden, ontstaan door implementatiefouten, in een van de fundamentele van het internet<sup>1</sup>: het Transmission Control Protocol, kortweg TCP. Dit protocol is een van de fundamentele protocollen voor de communicatie over netwerken, en dus ook het internet. Een grote verscheidenheid aan TCP implementaties blijkt kwetsbaar. Deze kwetsbaarheden zijn al in oktober 2008 ontdekt, maar gezien de aard en omvang van het probleem was het noodzakelijk leveranciers de tijd te geven hun implementaties te controleren. Naar verwachting zullen de komende tijd nog vele leveranciers patches uitbrengen waarmee deze kwetsbaarheden in het TCP protocol worden verholpen.

Deze factsheet zet de nu bekende feiten rondom deze kwetsbaarheden op een rij en draagt adviezen aan die kunnen helpen om de kans op misbruik van deze kwetsbaarheden te verkleinen of de impact ervan te beperken.

**Wat is er aan de hand?**

In oktober 2008 maken onderzoekers Jack Louis en Robert Lee van de firma Outpost24 bekend dat ze diverse kwetsbaarheden hebben ontdekt in verschillende TCP implementaties. Deze implementatiefouten stellen een kwaadwillende in staat om een Denial of Service aanval uit te voeren. Nieuw is dat deze aanval uitgevoerd kan worden met zeer weinig middelen en nauwelijks netwerkbandbreedte vergt. Dit in tegenstelling tot de meeste tot nu bekende (d)DOS aanvallen<sup>2</sup>. Er worden nog geen details bekend gemaakt en men speculeert volop of dit eigenlijk wel een (nieuw) probleem is. Aangezien TCP bij een enorme verscheidenheid van toepassingen gebruikt wordt, worden de gevolgen mede bepaald door de aard van de toepassing. Vanwege de potentieel grote impact wordt besloten het patchproces zo gecoördineerd als mogelijk te laten verlopen. CERT-FI<sup>3</sup> neemt hierin de leiding en geeft in hun advisory een overzicht van leveranciers die patches beschikbaar hebben. Deze advisory kunt u vinden via: <https://www.cert.fi/haavoittuvuudet/2008/tcp-vulnerabilities.html>

In november 2008 demonstrieren de onderzoekers de aanval ook aan medewerkers van GOVCERT.NL en is bevestigd dat het probleem ook echt en nieuw is.

**De belangrijkste feiten op een rij**

- > Er bevinden zich implementatiefouten in veel TCP implementaties. TCP is een van de basisprotocollen voor netwerkcommunicatie.
- > Detailgegevens zijn (nog) niet openbaar.
- > Op dit moment is er (nog) geen exploitcode publiek beschikbaar, maar met het beschikbaar komen van de patches wordt dit op korte termijn wel verwacht.
- > Misbruik kan leiden tot het op relatief eenvoudige wijze, en zonder al te veel inspanning, kunnen uitvoeren van een Denial of Service aanval. Het resultaat daarvan is dat communicatie en/of (web)diensten uitvallen.
- > Verschillende leveranciers hebben updates uitgebracht om de kwetsbaarheid in hun TCP implementatie te verhelpen.
- > Controleren op kwetsbare implementaties en zondig patchen zijn de belangrijkste acties die organisaties kunnen nemen om risico's te beperken.

<sup>1</sup> Meer over andere kwetsbaarheden in de fundamentele van het internet kunt u lezen in het GOVCERT.NL trendrapport 2009, te vinden op [www.govcert.nl](http://www.govcert.nl)

<sup>2</sup> Meer informatie over (d)DOS aanvallen kunt u lezen in het govcert whitepaper 'Aanvallen ter bescherming tegen DOS aanvallen'. Dit whitepaper kunt u downloaden via <http://www.govcert.nl/render.html?it=50>. Dit whitepaper geeft meer informatie over DOS aanvallen maar houdt geen rekening met de in dit factsheet beschreven techniek!

<sup>3</sup> CERT-FI is het Nationale CERT (Computer Emergency Response Team) van Finland.

## De “kwetsbaarheden”

Op het internet wordt het TCP/IP protocol gebruikt om gegevens uit te wisselen tussen systemen en applicaties. Om een verbinding tussen bijvoorbeeld een cliënt en server op te zetten, gebruikt TCP een "three-way handshake". Tijdens het 'TCP sockstress' onderzoek is gebleken dat de systeem bronnen, ten behoeve van een via "three way handshake" geïnitieerde TCP sessie, te misbruiken zijn. Deze systeem bronnen zijn onder andere tellers, timers en beschikbaar geheugen op kernel-niveau. Door een variatie aan aanvallen, zoals verschillende grootte van de 'window size', is het mogelijk om beschikbare resources permanent te reserveren. Via een handigheidje administreert de aanvaller deze connecties zodanig, dat dit de aanvaller vrijwel geen resources kost. Het gevolg is dat een applicatie, of zelfs het besturingssysteem, instabiel en onbereikbaar wordt. Hierdoor raakt een applicatie of systeem permanent of tijdelijk onbereikbaar. Permanente problemen op applicatieniveau zijn via een herstart van de applicatie op te lossen. Voor permanente problemen op besturingssysteemniveau is een herstart van het volledige systeem noodzakelijk. De impact bij misbruik van de kwetsbaarheden is verschillend per applicatie en per platform.

Door de beperkte benodigde bandbreedte is het moeilijk om de aanval te detecteren, vooral omdat het netwerkverkeer op gewoon legitiem netwerkverkeer lijkt. Met minimale middelen aan computerkracht en bandbreedte kan een aanvaller dus ernstige problemen veroorzaken op servers (zoals web- en ftp servers) en infra-componenten (zoals routers, firewalls, switches).

TCP sockstress aanvallen zijn niet nieuw<sup>4</sup>. Wat wel nieuw is, is dat er maar zeer beperkte resources nodig zijn voor deze variant.

## Wat is de impact van de kwetsbaarheid?

De algehele impact bij misbruik van de kwetsbaarheden is een Denial of Service. De mate van de impact is afhankelijk van de aard applicatie, en het besturingssysteem waarop de applicatie draait.

De mate van de impact is te verdelen in 3 categorieën:

### 1. Tijdelijke impact op de applicatie

De applicatie accepteert tijdelijk geen nieuwe verbindingen ten tijde van de aanval. Wanneer de aanval wordt beëindigd, is de applicatie weer in een bruikbare staat en dus weer bereikbaar.

### 2. Permanente impact op de applicatie

De applicatie accepteert geen nieuwe verbindingen wanneer de aanval wordt ingezet. De applicatie blijft vervolgens in deze permanente staat, ook wanneer de aanval wordt beëindigd. Een herstart van de applicatie lost vervolgens het probleem op.

### 3. Permanente impact op het besturingssysteem

De kernel van het besturingssysteem is niet meer in staat om essentiële taken uit te voeren wanneer de aanval wordt ingezet. Het resultaat is dat het systeem volledig onbruikbaar wordt. Een herstart van het systeem is in dit geval de enige oplossing.

---

<sup>4</sup> In juni 2009 beschreef Prack magazine een andere methode voor het uitvoeren van een DoS aanval op TCP (<http://www.phrack.com/issues.html?issue=66&id=9#article>). Dat artikel beschrijft niet exact hetzelfde, maar wel een soortgelijk probleem.

## Wat kunt u eraan doen?

De vraag is welke acties uw organisatie moet uitvoeren om de kans op misbruik van deze kwetsbaarheid te verkleinen. Onderstaand volgen de belangrijkste acties die u kunt overwegen:

1. Stap één is te inventariseren of uw organisatie een kwetsbare TCP implementatie gebruikt. Helaas is momenteel slechts door een klein aantal leveranciers bekend gemaakt of hun producten kwetsbaar zijn, en indien van toepassing, er patches beschikbaar zijn gesteld. Er is momenteel een groot aantal leveranciers aan het onderzoeken of hun producten kwetsbaar zijn. De mogelijke kwetsbaarheden kunnen zich dus uitstrekken over een grote variatie in applicaties en besturingssystemen. CERT-FI houdt een leveranciersoverzicht bij, dit is te vinden op <https://www.cert.fi/haavoittuvuudet/2008/tcp-vulnerabilities.html>  
US-CERT heeft een overzicht gepubliceerd van alle leveranciers die geïnformeerd zijn, inclusief de laatst bekende status (onbekend, kwetsbaar, niet-kwetsbaar). Dit overzicht is te vinden op <http://www.kb.cert.org/vuls/id/723308>
2. Er is nog geen tooling beschikbaar om zelf te onderzoeken of uw implementaties kwetsbaar zijn. Er is wel tooling beschikbaar gesteld aan leveranciers.
3. Mocht uit uw inventarisatie blijken dat uw TCP implementatie kwetsbaar is, dan is het zaak deze zo snel mogelijk te patchen. U kunt hiervoor de informatie uit GOVCERT.NL advisory 2009-255<sup>5</sup> gebruiken.
4. Mocht het niet mogelijk zijn om te patchen, dan kunt u kijken of tegenmaatregelen, zoals beschreven in de Engelstalige paper: " Security assesment of the TCP protocol", voor uw organisatie en situatie van toepassing kunnen zijn. Deze paper kunt u vinden op de website van het Britse Centre for the Protection of National Infrastructure (CPNI) <http://www.cpni.gov.uk/Products/technicalnotes/Feb-09-security-assessment-TCP.aspx>
5. Blijf alert op het uitbrengen van security patches door uw leveranciers. Naar verwachting zullen een aantal leveranciers patches uitbrengen voor deze kwetsbaarheden.

## Inmiddels uitgebrachte patches, leveranciersoverzicht (stand per 7 december 2009):

Diverse leveranciers zullen de komende tijd patches uitbrengen indien hun platformen kwetsbaar zijn. CERT-FI, onze Finse partner die de coördinatie over deze kwetsbaarheid heeft, beschrijft in hun advisory de laatste stand van zaken betreffende leveranciers die patches beschikbaar hebben gesteld, danwel leveranciers die aangeven niet kwetsbaar te zijn. Deze advisory kunt u vinden via:

<https://www.cert.fi/haavoittuvuudet/2008/tcp-vulnerabilities.html>

De volgende leveranciers hebben inmiddels updates beschikbaar gesteld. We raden u aan om deze updates te installeren.

### Aruba

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

### Bluecoat

Diverse Bluecoat producten zijn kwetsbaar. Nadere informatie kunt u vinden op de Bluecoat website, (een geldig login voor deze site is benodigd)

<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>

<sup>5</sup> GOVCERT.NL advisories zijn alleen beschikbaar voor deelnemers.

### *Checkpoint*

[https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit\\_doGoviewsolutiondetails=&solutionid=sk42723](https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk42723)  
[https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit\\_doGoviewsolutiondetails=&solutionid=sk42725](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*

De mail en web security appliance software is kwetsbaar.

<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 heeft aangegeven dat VX Works kwetsbaar is

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

De volgende leveranciers hebben aangegeven dat hun producten kwetsbaar zijn. Zij hebben echter (nog) geen patch ter beschikking gesteld.

### *Juniper*

Juniper heeft bevestigd dat hun apparatuur kwetsbaar is. Echter, Juniper beschouwt de beschreven kwetsbaarheden als generieke, eerder gepubliceerde aanvallen op het TCP protocol. Daarvoor adviseert Juniper om de 'best common practices' die zij eerder hebben gepubliceerd op te volgen. Informatie hierover vindt u in de volgende Juniper advisory:

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

### *Red Hat*

Red Hat heeft aangegeven dat Red Hat Enterprise Linux wel kwetsbaar is, maar dat Red Hat geen updates voor dit OS zal uitbrengen. <http://kbase.redhat.com/faq/docs/DOC-18730>

### *SUSE*

SUSE heeft aangegeven dat SUSE Linux kwetsbaar is maar er zal geen update voor worden uitgebracht. [http://www.novell.com/linux/security/advisories/2009\\_47\\_tcpip.html](http://www.novell.com/linux/security/advisories/2009_47_tcpip.html)

### *Sun microsystems*

Sun heeft bevestigd dat een aantal van hun producten kwetsbaar is. Een patch is nog niet beschikbaar gesteld. Meer informatie vindt u bij <http://sunsolve.sun.com/search/document.do?assetkey=1-66-267088-1>

### *Stonesoft*

Stonesoft heeft aangegeven dat bepaalde versies van hun producten kwetsbaar zijn. Er zijn nog geen updates beschikbaar: [http://www.stonesoft.com/en/support/security\\_advisories/2009\\_17\\_09.html](http://www.stonesoft.com/en/support/security_advisories/2009_17_09.html)

De volgende leveranciers hebben aangegeven niet kwetsbaar te zijn:

### *Clavister*

Clavister heeft aangegeven niet kwetsbaar te zijn

### *Fortinet*

Fortinet heeft aangegeven niet kwetsbaar te zijn

### *VMWare*

VMWare heeft aangegeven niet kwetsbaar te zijn