

Risico analyse m.b.t. de zogenaamde TCP sockstress DoS attack security alert.

De door Outpost24 in oktober 2008 ontdekte en daarna door CERT Finland begeleide kwetsbaarheid in de TCP-stack van op basis van IP communicerende apparatuur, heeft een beperkt risicobereik. Om te bepalen of apparatuur tot de risicogroep behoort stellen wij hier enkele controle toetsen op.

Aard van de kwetsbaarheid.

Een TCP sockstress Denial of Service aanval kenmerkt zich door het beperkte verkeer dat hiervoor nodig is. Het gaat slechts om een TCP-handshake procedure. Hierin zit ook direct het risico bepalende element opgesloten:

Alleen interfaces van apparaten waarop een TCP-verbinding kan worden "getermineerd" zijn kwetsbaar. Interfaces die TCP-verkeer transparant doorzetten zijn dus NIET kwetsbaar.

Risicogroep.

1. Alle randapparatuur (vooral servers) waarmee via TCP verbinding kan worden gemaakt behoort tot de risicogroep.
2. Alle netwerkkapparatuur waarmee via TCP verbinding kan worden gemaakt behoort tot de risicogroep:
 - a. VPN-gateways die via TCP worden benaderd vanuit een IPsec client kunnen via deze (vertrouwde tunnel-)verbindingen kwetsbaar zijn. Wordt UDP hiervoor gebruikt, dan zijn deze gateways niet kwetsbaar.
 - b. Switches en routers die via TCP worden beheerd zijn alleen kwetsbaar op interfaces die beheer toelaten. Deze beheerinterfaces zijn vaak afgeschermd voor gebruikers, het betreft meestal dus de specifieke management-(VLAN-)interfaces.
 - c. Firewalls worden meestal alleen vanuit het "trusted" netwerk beheerd. Alleen trusted interfaces die TCP verbindingen tbv. beheer ondersteunen zijn mogelijk kwetsbaar.
 - d. Overige netwerkkapparatuur is alleen mogelijk kwetsbaar op interfaces die TCP verbindingen ondersteunen, hoofdzakelijk zijn dit interfaces voor beheer doeleinden.
3. Alle netwerkkapparatuur-interfaces die TCP transparant doorlaten, zijn dus NIET kwetsbaar.

Workaround.

Blijkt een apparaat kwetsbaar conform de opgave van de fabrikant (alleen die kan dit aangeven), dan kunnen risico interfaces worden afgeschermd door deze achter een IPS (met Virtual Patching) te plaatsen of door ACLs (filters) op de betreffende interfaces in te stellen.

Upgrade.

Apparatuur die door de fabrikant als kwetsbaar wordt aangeduid, kan via een software upgrade immuun worden gemaakt voor de hier beschreven kwetsbaarheid. De fabrikant geeft in dat geval aan, vanaf welke softwareversie de apparatuur immuun is. Apparatuur met een laag risico kan tijdens reguliere change-windows worden aangepast.

Informatie.

Vosko houdt u via haar website op de hoogte van deze alert, de directe URL is: www.vosko.nl/tcp

Voor meer informatie: Vosko Networking BV, tel: 0182622822, email: info@vosko.nl

In het vertrouwen u van dienst te zijn geweest, Wim Coenen / Teamleader Security Task Force.