

Beste klant

De internetworm 'Downadup' (Conficker) verspreidt zich explosief. VirusAlert.nl heeft daarom het waarschuwingsniveau verhoogd en vandaar deze nieuwsbrief.

De worm kan zich nestelen op alle Windows-systemen en maakt daarvoor ondermeer gebruik van een lek in Windows. Het is daarom zaak om uw Windows-systeem z.s.m. te updaten met de laatste reparatie-software.

Dit kunt u binnenhalen via Windows Update.

### **W32.Downadup (Conficker) (Internet Worm)**

Besturing: Microsoft Windows

Datum: 18 januari 2009

Risico: Hoog

Bron: (c) 2009, VirusAlert

Worm: Win32/Conficker.A

Crypt.AVL

Mal/Conficker-A

Trojan.Win32.Pakes.lxf

Trojan.Win32.Pakes.lxf

W32.Downadup

Worm: Win32/Conficker.B

WORM\_DOWNAD.A

Eigenschappen:

**Downadup** is een internetworm die zich verspreidt via een lek in de Windows-software. Dit lek bevindt zich in het Server Message Block Protocol wat gebruikt wordt voor het delen van bestanden en printers.

Meer informatie over dit lek vindt u bij Microsoft.

Microsoft Security Bulletin MS08-067 – Critical

Vulnerability in Server Service Could Allow Remote Code Execution (958644)

Published: October 23, 2008

Na infectie installeert het een aantal bestanden op het systeem en afhankelijk van de versie van Downadup verricht het acties als;

- Het blokkeren van de toegang tot antiviruswebsites
- Het verzamelen van gegevens voor online games
- Installeert een HTTP service op het getroffen systeem om zodoende de worm verder te verspreiden