

# FACTSHEET FS-2008-07

## Achtergrondinformatie over Microsoft update MS08-067

Op donderdag 23 oktober 2008 bracht Microsoft een patch uit voor een ernstige kwetsbaarheid in alle versies van Windows. Bijzonder is dat deze patch buiten de reguliere patch-cyclus om werd uitgebracht. De reden hiervoor is dat Microsoft de kwetsbaarheid als bijzonder ernstig inschaalt en dat kwaadwillenden de kwetsbaarheid al actief uitbuiten.

GOVCERT.NL heeft haar deelnemers in beveiligingsadvies GOVCERT.NL-2008-353 direct ingelicht over deze ontwikkeling<sup>1</sup>. Dat beveiligingsadvies bevat informatie over de kwetsbaarheid en mogelijkheden om de impact ervan te minimaliseren.

Na het uitkomen van de patch publiceerden diverse bronnen meer informatie over de kwetsbaarheid en het misbruik ervan. Deze factsheet brengt deze informatie samen om u te helpen de impact van deze kwetsbaarheid voor uw eigen organisatie in te schatten en acties te ondernemen om de impact te minimaliseren.

### De belangrijkste feiten op een rij:

- > Update MS08-067 dicht een lek in de Windows Server service dat actief wordt misbruikt.
- > Alle versies van Windows zijn kwetsbaar.
- > GOVCERT.NL raadt u aan om de patch zo snel mogelijk te testen en te installeren.
- > Uitbuiten van de kwetsbaarheid kan uitsluitend via poort 139/tcp of 445/tcp.
- > De Conficker-worm heeft via deze kwetsbaarheid een groot aantal PC's geïnfecteerd.

### Aard en impact van de kwetsbaarheid

De ontdekte kwetsbaarheid bevindt zich in de 'Windows Server' service welke op alle ondersteunde Windows-versies aanwezig is. Succesvol misbruik van de kwetsbaarheid leidt in veel gevallen tot het uitvoeren van willekeurige code onder SYSTEM rechten. Het SYSTEM account van Windows heeft dezelfde rechten als een beheerder (administrator) waardoor de mogelijkheden die kwaadwillenden hebben enorm zijn.

De impact van de kwetsbaarheid en de kans op misbruik verschillen echter wel per besturingssysteem. In de tabel hieronder is een overzicht opgenomen van de impact van de kwetsbaarheid en mitigerende factoren per Windows-versie.

#### Impact per versie van Windows

Versie	Impact	Mitigerende factoren
NT4 (*)	Onbekend. Waarschijnlijk code-executie.	
Windows 2000	Code-executie zonder autorisatie	
Windows XP	Code-executie zonder autorisatie	Standaard Windows firewall blokkeert inkomend verkeer naar betreffende poorten.
Windows server 2003	Code-executie zonder autorisatie	
Windows Vista	Waarschijnlijk alleen DoS. Autorisatie benodigd.	Windows firewall blokkeert inkomend verkeer naar betreffende poorten. DEP en ASLR maken uitbuiting moeilijk.
Windows server 2008	Waarschijnlijk alleen DoS. Autorisatie benodigd.	Windows firewall blokkeert inkomend verkeer naar betreffende poorten. DEP en ASLR maken uitbuiting moeilijk.

(\*) NT4 wordt sinds 1 januari 2005 niet meer ondersteund door Microsoft, tenzij u een *Custom Support* overeenkomst heeft afgesloten. Neem voor vragen contact op met uw contactpersoon bij Microsoft.

Een belangrijk onderscheid tussen de verschillende versies van Windows is dat onder Windows Server 2008 en Windows Vista autorisatie vereist is om een verbinding te maken met de Windows Server service. Bij alle andere versies van Windows kan anoniem een verbinding worden opgezet.

<sup>1</sup> GOVCERT.NL beveiligingsadviezen zijn alleen beschikbaar voor deelnemers van GOVCERT.NL

Daarnaast ziet u in het overzicht dat de Windows firewall die standaard op Windows XP, Vista en Server 2008 aanwezig is, de betreffende systemen beschermt. Uiteraard is dit alleen het geval als de firewall ook daadwerkelijk aan staat. Daarnaast zijn er nog enkele scenario's waarbij configuratiewijzigingen op deze versies van Windows ervoor zorgen dat gebruikers toch kwetsbaar zijn:

- Een XP-station is opgenomen in een Windows-domein. Afhankelijk van de configuratie kan dit ertoe leiden dat de standaard firewall-instellingen worden gewijzigd.
- Op een XP-station is File and Printer Sharing of Simple File Sharing ingeschakeld. Daarbij zal Windows XP binnenkomend verkeer naar de poorten 139/tcp en 445/tcp doorlaten.
- Op een Vista-station is File and Printer Sharing ingeschakeld. Bij deze configuratie zal Windows Vista binnenkomend verkeer naar de poorten 139/tcp en 445/tcp alleen toestaan voor het 'Private' netwerk. Ook hier is bovendien weer succesvolle authenticatie benodigd.
- Onder Vista kunnen gebruikers er ook voor kiezen om bestanden te delen met de optie Password Protected Sharing Disabled. In dit geval is er geen authenticatie meer benodigd om de kwetsbaarheid te kunnen misbruiken.

### Gedetailleerde informatie over de kwetsbaarheid

De ontdekte ernstige kwetsbaarheid bevindt zich in de Windows-functie 'NetPathCanonicalize', die onderdeel uitmaakt van het bibliotheekbestand NETAPI32.DLL<sup>2</sup>. Kwaadwillenden kunnen deze kwetsbaarheid misbruiken via de Microsoft Windows Server Service. Misbruik vindt plaats met malafide 'Remote Procedure Calls' (RPC) over SMB (Server Message Blocks).

SMB maakt het mogelijk om via het netwerk toegang te verkrijgen tot bestanden, printers en andere bronnen op een systeem. Wanneer een client via SMB een bestand (of een andere gedeelde bron) wil benaderen, opent deze een zogenaamde *named pipe* naar de bron. De *named pipe* heeft een structuur die veel weg heeft van een directorypad.

De Windows Server service maakt gebruik van de functie 'NetPathCanonicalize' om deze paden (bijvoorbeeld \Temp) te normaliseren. Bevindt er zich in een padnaam een verwijzing naar een parent directory ('..'), dan betekent dit dat Windows een niveau hoger in de boomstructuur moet gaan. Een pad als '\\A\B\..\C' normaliseert de eerder genoemde functie dan ook tot '\\A\C'. Om deze normalisatie uit te kunnen voeren, zoekt de functie vanaf de plek waar de '..' voorkomt, terug naar de vorige backslash in het pad. Wanneer er meerdere verwijzingen achter elkaar voorkomen (bijvoorbeeld '\\..\..') dan doet de functie dit meerdere keren. Er doet zich echter een probleem voor wanneer opeenvolgende parent directory verwijzingen ervoor zorgen dat de functie buiten de top van de boomstructuur treedt. Dit kan gebeuren bij een pad zoals onderstaand weergegeven:

```
'\\A\..\..\C'
```

Het normaliseren van bovenstaand pad is in principe niet mogelijk aangezien '\\A\..' al verwijst naar de root ('\') en men vanuit daar dus niet nog een niveau hoger in de boomstructuur kan gaan. Onderzoekers van het bedrijf ImmunitySec hebben beschreven dat er in dit geval een foutieve berekening plaatsvindt waardoor de functie vanaf 1 byte vóór het eerste karakter in de buffer op zoek gaat naar deze backslash. Door te zorgen dat er vóór het uitvoeren van de functie al een dergelijke backslash op de stack voorkomt, zou men de ontstane stack underflow succesvol kunnen misbruiken<sup>3</sup>. Volgens Microsoft ontstaat er bij het normaliseren een stack-based buffer overflow binnen een loop<sup>4</sup>.

De kwetsbaarheid kan alleen misbruikt worden via de poorten 139/tcp (NetBIOS) en 445/tcp (CIFS). Het probleem bevindt zich dan ook niet in RPC maar in SMB. Het is dus niet mogelijk om de kwetsbaarheid uit te buiten via bijvoorbeeld RPC over HTTP.

Binnen 2 uur na het beschikbaar komen van de Microsoft-update, bood het bedrijf ImmunitySec al een exploit aan aan betalende klanten van deze organisatie<sup>5</sup>. In de dagen daaropvolgend verschenen ook exploits op publieke websites als Milw0rm en SecurityFocus<sup>6</sup>. In eerste instantie was de gepubliceerde code nog niet bruikbaar voor een betrouwbare aanval<sup>7</sup>. Op 27 oktober gaf Microsoft echter aan dat publiek beschikbare code succesvol misbruikt kan worden voor het uitvoeren van willekeurige code op Windows 2000, XP en 2003<sup>8</sup>.

<sup>2</sup> <http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4250>

<sup>3</sup> [http://media.haymarketmedia.com/Documents/1/Alrighy%20so%20what%20happens%20is\\_856.pdf](http://media.haymarketmedia.com/Documents/1/Alrighy%20so%20what%20happens%20is_856.pdf)

<sup>4</sup> <http://blogs.technet.com/msrc/archive/2008/10/27/microsoft-out-of-band-security-bulletin-ms08-067-webcast-q-a.aspx>

<sup>5</sup> <http://www.scmagazineus.com/Separate-proofs-of-concept-released-after-rushed-Windows-fix/article/119925/>

<sup>6</sup> <http://www.securityfocus.com/bid/31874>

<sup>7</sup> <http://blogs.technet.com/msrc/archive/2008/10/26/update-on-ms08-067.aspx>

<sup>8</sup> <http://www.microsoft.com/technet/security/advisory/958963.msp>

## Bescherming tegen de kwetsbaarheid

De beste bescherming tegen misbruik van deze kwetsbaarheid vormt uiteraard het installeren van de update van Microsoft (MS08-067)<sup>9</sup>.

Gebruikers van Windows NT4 kunnen het probleem alleen verhelpen wanneer zij een *NT4 Custom Support Agreement* met Microsoft hebben afgesloten. Via dit contract distribueert Microsoft patches voor Windows NT4 Server, NT4 Workstation en NT4 Terminal Server.

Mocht het niet mogelijk zijn om de patch op korte termijn te installeren dan bestaan nog een aantal workarounds om de kans op misbruik te verkleinen. Deze vindt u in de tabel hiernaast.

## Kwetsbare systemen detecteren

Alle Windows systemen binnen uw netwerk die niet voorzien zijn van de MS08-067 patch zijn kwetsbaar. Om inzicht te krijgen in de systemen die op dit moment nog kwetsbaar zijn, kunt u het beste gebruik maken van de standaard Windows tools zoals Windows Software Update Services (WSUS).

Aanvullend kunt u een scan uitvoeren op basis van bijvoorbeeld Nessus. Nessus is een *vulnerability scanner* die het netwerk kan afschannen op zoek naar kwetsbare systemen. Voor deze kwetsbaarheid heeft Nessus twee plugins ontwikkeld<sup>10</sup>:

- Plugin #34476<sup>11</sup>: deze plugin voert een grondige scan uit naar alle kwetsbare systemen in het netwerk. De plugin voert een analyse uit op aanwezige DLL's op het systeem en kan op die manier vaststellen dat er gebruik gemaakt wordt van kwetsbare bibliotheken. Op deze manier krijgt men ook inzicht in systemen die wel gepatched zijn maar nog niet zijn herstart. Voor deze plugin moet men credentials opgeven.
- Plugin #34477<sup>12</sup>: deze plugin kan men gebruiken om een snelle scan uit te voeren naar kwetsbare systemen. De plugin maakt verbinding met de poorten 139/tcp en 445/tcp om vast te stellen of het systeem kwetsbaar is. Deze plugin kan men uitvoeren zonder hiervoor credentials op te geven.

## Geïnficeerde systemen en misbruik detecteren

Om geïnficeerde systemen binnen uw netwerk op te sporen bestaan verschillende mogelijkheden:

- Controleer meldingen van uw virusscanners. Met name de aanwezigheid van bepaalde malware duidt op misbruik van de kwetsbaarheid. Zie meer informatie hierover onder het kopje 'Worm en gerelateerde malware' op de volgende pagina.
- Controleer uitgaand netwerkverkeer op basis van de domeinen waarmee nu bekende malware probeert te verbinden. Een (poging tot) verbinding vanuit uw netwerk met één van deze domeinen is een indicatie dat een systeem op uw netwerk besmet is. Met name interessant is in dit geval de lijst met domeinnamen waarvan de Conficker-worm gebruik maakt<sup>13</sup>. Ook toegenomen activiteit op de poorten 139/tcp en 445/tcp kan duiden op besmetting.
- Configureer uw intrusion detection systems (IDS) om de betreffende aanvallen en exploits te kunnen detecteren. Een IDS zal voor het detecteren van aanvallen op zoek gaan naar de RPC Identifier (UUID) voor de Windows Server Service (4b324fc8-1670-01d3-1278-5a47bf6ee188)<sup>14</sup> en dit combineren met herkenning van een opeenvolging van parent directory verwijzingen (bijvoorbeeld '..\..'). De manier waarop u uw IDS moet configureren is veelal afhankelijk het type IDS dat u gebruikt. Cisco, bijvoorbeeld, heeft een apart document opgesteld<sup>15</sup> waarin staat beschreven op welke manier u Cisco-componenten kunt configureren. Voor Snort bestaan verschillende rules: gratis rules van EmergingThreats<sup>16</sup> of de betaalde rules van SourceFire<sup>17</sup>.

## Mogelijke workarounds:

Voor alle workarounds geldt: bepaal en test de impact van de workaround voordat u deze implementeert.

- > Blokkeer toegang tot poorten 139/tcp en 445/tcp. Doe dit niet alleen vanaf het internet naar uw interne netwerk, maar ook tussen onderlinge segmenten op uw interne netwerk. Hiermee voorkomt u dat wormen zich onbeperkt op uw interne netwerk kunnen verspreiden.
- > Schakel de Windows Server service en de Browser service uit. Werkstations hebben deze services over het algemeen niet nodig. Servers daarentegen zijn voor het correct functioneren veelal afhankelijk van deze services.
- > Voer maatregelen door om misbruik van de kwetsbaarheid te detecteren. Meer hierover kunt u terugvinden onder het kopje 'Geïnficeerde systemen en misbruik detecteren'.

<sup>9</sup> Meer informatie kunt u vinden op <http://www.microsoft.com/technet/security/bulletin/MS08-067.mspx>

<sup>10</sup> <http://blog.tenablesecurity.com/2008/10/network-and-cre.html>

<sup>11</sup> <http://www.nessus.org/plugins/index.php?view=detail&id=34476>

<sup>12</sup> <http://www.nessus.org/plugins/index.php?view=detail&id=34477>

<sup>13</sup> [http://www.cert.at/static/conficker/all\\_domains.txt](http://www.cert.at/static/conficker/all_domains.txt)

<sup>14</sup> <http://tools.cisco.com/security/center/viewAlert.x?alertId=16941>

<sup>15</sup> <http://tools.cisco.com/security/center/viewAlert.x?alertId=16944>

<sup>16</sup> [http://www.emergingthreats.net/cgi-bin/cvsweb.cgi/signs/EXPLOIT/EXPLOIT\\_MS08-067](http://www.emergingthreats.net/cgi-bin/cvsweb.cgi/signs/EXPLOIT/EXPLOIT_MS08-067)

## Worm en gerelateerde malware

Microsoft onderkende vanaf de publicatie van het beveiligingsadvies dat de kwetsbaarheid uit te buiten is door een worm die zich zelf kan verspreiden. Dat is dan ook één van de redenen waarom de patch buiten de gangbare patchcyclus werd uitgebracht. De kwetsbaarheid is aanwezig op alle Windows-systemen en kan worden misbruikt zonder dat daarvoor gebruikersinteractie benodigd is.

In eerste instantie leek het met malware en wormen die misbruik maakten van de kwetsbaarheid nog mee te vallen. Kort na het bekendmaken van de kwetsbaarheid werd weliswaar malware genaamd 'Gimmiv' ontdekt die daar misbruik van maakte, maar die verspreidde zich uiteindelijk slechts beperkt.

Echter, op 25 november 2008, ruim een maand na het uitkomen van de patch, meldde Microsoft dat het steeds meer meldingen ontving van een ernstigere worm die het lek actief uitbuitte<sup>18</sup>. De worm is inmiddels bekend geworden onder verschillende namen waaronder Conficker<sup>19</sup>, Conficker<sup>20</sup>, Downadup<sup>21</sup> en Kido<sup>22</sup>.

De Conficker worm maakt onder andere misbruik van de MS08-067 kwetsbaarheid om andere systemen binnen een netwerk te besmetten. Eenmaal geïnfecteerd past Conficker de TCP/IP-instellingen op de PC aan om in een zo kort mogelijk tijdsbestek zoveel mogelijk systemen te kunnen besmetten.

Misbruik van de MS08-067 kwetsbaarheid is echter niet de enige manier waarop Conficker een PC infecteert. Zo verspreidt de worm zich ook via USB-sticks en probeert het om verbinding te maken met netwerk shares op basis van zwakke wachtwoorden. Dit laatste kan ertoe leiden dat gebruikersaccounts op een systeem plotseling 'locked out' raken door het grote aantal pogingen van de worm om zich aan te melden op basis van een standaard lijst van wachtwoorden. Een eenmaal geïnfecteerde PC binnen het netwerk kan dus op verschillende manieren andere systemen binnen het netwerk infecteren.

Op verschillende manieren voorkomt Conficker dat een gebruiker de worm weer van zijn PC verwijderd. Zo schakelt de worm enkele essentiële Windows-services uit waardoor updates niet meer automatisch op het systeem worden geïnstalleerd. Ook zorgt Conficker ervoor dat de gebruiker bepaalde websites niet meer kan benaderen wanneer in de naam van de website een bepaald sleutelwoord voorkomt. Hierdoor kan een gebruiker bijvoorbeeld de Malicious Software Removal Tool (MSRT) van Microsoft niet meer downloaden om via deze tool de worm te verwijderen. Om gebruikers van geïnfecteerde PC's toch de mogelijkheid te bieden om gebruik te maken van deze tool, biedt onder meer [Waarschuwingsdienst.nl](http://www.waarschuwingsdienst.nl) een kopie van de tool aan via haar website<sup>23</sup>.

Opvallend aan Conficker is dat het na infectie gebruik maakt van pseudo-willekeurige domeinnamen om aanvullende bestanden te downloaden. Per dag maakt Conficker gebruik van zo'n 250 verschillende domeinnamen. Het 'uit de lucht halen' van een specifiek domein zal dus niet helpen om de worm een halt toe te roepen. Aan de andere kant biedt het malware onderzoekers ook een groot aantal mogelijkheden. Aangezien het algoritme voor het genereren van domeinnamen kon worden gekraakt, was het mogelijk om op voorhand domeinnamen te registreren en verkeer vanaf geïnfecteerde PC's naar een eigen server te routeren. Op die manier was het mogelijk om inzicht te krijgen in de hoeveelheid systemen die door Conficker getroffen zijn. Volgens verschillende anti-virusleveranciers loopt het aantal infecties wereldwijd in de vele miljoenen waarbij vooral Azië en Zuid-Amerika getroffen lijken te zijn.

### Conficker highlights

- > Verspreidt zich via geïnfecteerde USB-sticks in combinatie met de Autorun feature van Windows, netwerk shares voorzien van zwakke wachtwoorden en ongepatchte Windows-systemen.
- > Schakelt verschillende belangrijke Windows-services uit zoals de 'Windows Security Center Service' en de 'Windows Update Auto Update Service'.
- > Voorkomt dat beveiligingsprogrammatuur in staat is om updates e.d. te downloaden.
- > Blokkeert de toegang tot websites met daarin bepaalde sleutelwoorden (zoals 'norton', 'etrust' en 'windowsupdate').
- > Probeert op de lokale gateway een firewall rule aan te maken die verkeer richting de geïnfecteerde PC toestaat.
- > Maakt gebruik van pseudo-willekeurige domeinnamen voor het downloaden van binaries.

<sup>17</sup> <http://www.snort.org/pub-bin/snortnews.cgi#819>

<sup>18</sup> <http://blogs.technet.com/mmpc/archive/2008/11/25/more-ms08-067-exploits.aspx>

<sup>19</sup> <http://www.microsoft.com/security/portal/Entry.aspx?Name=Worm%3aWin32%2fConficker.B>

<sup>20</sup> <http://www.pandasecurity.com/homeusers/security-info/about-malware/encyclopedia/overview.aspx?IdVirus=202881>

<sup>21</sup> [http://www.symantec.com/security\\_response/writeup.jsp?docid=2008-112203-2408-99&tabid=1](http://www.symantec.com/security_response/writeup.jsp?docid=2008-112203-2408-99&tabid=1)

<sup>22</sup> <http://www.viruslist.com/en/viruses/encyclopedia?virusid=21782749>

<sup>23</sup> <http://www.waarschuwingsdienst.nl/render.html?it=1896>