
# Informatie over Meltdown en Spectre problemen met betrekking tot door Coblin geleverde systemen

versie 180111A
11 januari 2018

# 1. Algemeen

Zoals wellicht bekend zorgen processorfouten, genaamd ‘Meltdown’ en ‘Spectre’, voor beveiligingsproblemen bij PC’s, smartphones, tablets, NAS systemen, firewalls en servers. Coblin informeert u hierbij over de actuele stand van zaken voor wat betreft desktops, laptops, NAS systemen en firewalls. Let op: Deze informatie betreft alleen de actuele stand van zaken, voor zover bekend. Zijn er vragen? Neem dan contact met ons op.

# 2. Advies te nemen maatregelen

| | |
|---|---|
| **Alle desktops en laptops** | |
| - | Windows, Linux: controleer of uw internetbrowsers (met name Firefox en Chrome) up-to-date zijn |
| - | Windows 7, 8, 8.1, Linux: controleer of er systeemupdates beschikbaar zijn en installeer deze |
| - | BIOS update uitvoeren of laten uitvoeren, indien beschikbaar. Maak van te voren een goede gegevens back-up. |
| **Desktops en laptops ouder dan 5 jaar** | |
| - | Zorg ervoor dat deze systemen geen toegang meer krijgen tot de GUI’s van NAS systemen, firewalls of randapparatuur (switches, routers, Access Points, printers etc.) |
| - | Zorg ervoor dat deze systemen geen toegang hebben tot vertrouwelijke gegevens, direct of indirect. Ook toegang tot cloud toepassingen vormen een risico. |
| **NAS systemen** | |
| - | Zorg ervoor dat alleen tegen Meltdown en Spectre beveiligde apparaten (PC’s, tablets, smartphones) toegang hebben tot de GUI |
| - | controleer uw back-ups of laat deze controleren |
| - | Netgear: installeer de nodige updates voor uw Netgear NAS op aanwijzing van de fabrikant. Herhaal de controle op updates regelmatig. |
| - | Coblin bNAS Pro: BIOS update uitvoeren of laten uitvoeren. Coblin informeert u over eventuele extra maatregelen zodra die nodig cq. bekend zijn. |
| | |
| **Coblin bSafe firewalls** | |
| - | Zorg ervoor dat alleen tegen Meltdown en Spectre beveiligde apparaten (PC’s, tablets, smartphones) toegang hebben tot de GUI |
| - | tot 5 jaar oud: BIOS update uitvoeren of laten uitvoeren |
| - | ouder dan 5 jaar: overweeg vervanging |
| **Overige randapparatuur (switches routers, printers etc.)** | |
| - | Zorg ervoor dat alleen tegen Meltdown en Spectre beveiligde apparaten (PC’s, tablets, smartphones) toegang hebben tot de GUI |
| - | informeer u via de website van de fabrikant van uw randapparatuur. Neem bij vragen contact op met Coblin. |

# 3. Kosten

Tenzij u een support contract met Coblin hebt afgesloten, is Coblin niet verantwoordelijk voor het up-to-date houden van geleverde apparatuur. De kosten voor aanpassingen ten gevolge van de Meltdown en Spectre problemen vallen dan ook buiten de garantie.

# 4. Maatregelen voor desktops en laptops

## 4.1 Software updates (patches)

Voor de besturingssystemen Microsoft Windows (vanaf Windows 7), Mac OS en Linux zijn inmiddels updates, ook wel patches genoemd, uitgebracht voor Meltdown en Spectre. Onder Windows 10 worden deze updates automatisch geinstalleerd. Dit geldt ook voor de browser *Microsoft Edge*. Ook andere browsers, zoals Firefox en Google Chrome, worden doorgaans automatisch geactualiseerd. Voor Firefox en Chrome is het wel verstandig om te controleren of u over de meest recente versie beschikt.

## 4.2 BIOS upgrade

Naast de software updates is een BIOS upgrade noodzakelijk. Voor de meeste PC's die niet ouder zijn dan 5 jaar zijn inmiddels BIOS upgrades uitgebracht. Een BIOS upgrade kan niet op afstand worden uitgevoerd; u kunt hiervoor uw PC bij Coblin laten upgraden. Het op lokatie upgraden is ook mogelijk, en wenselijk wanneer u ook over een NAS systeem beschikt. Een goede back-up van de gegevens op uw PC is belangrijk. De kosten voor een BIOS upgrade bedragen € 40,- excl. btw / € 48,40 incl. btw per PC.

## 4.3 Systemen ouder dan 5 jaar

Intel, de fabrikant waarop alle geleverde Coblin  desktops en laptops zijn gebaseerd, heeft aangegeven dat voor systemen die minder dan 5 jaar oud zijn een BIOS update beschikbaar komt om de problemen door Meltdown en Spectre op te lossen. Voor systemen ouder dan 5 jaar heeft Intel nog geen oplossing aangeboden, waarmee deze systemen voorlopig kwetsbaar blijven voor Meltdown en Spectre. Bij systemen waarop geen BIOS upgrade is uitgevoerd en die toegang hebben tot de GUI van NAS systemen, firewalls, printers, routers etc, is het risico op problemen aanwezig. Ook het uitvoeren van bankzaken of het inloggen op cloudgebaseerde programma's is risicovol.

# 5. Maatregelen voor NAS systemen

## 5.1 Beveilig apparaten die toegang hebben

Apparaten (PC's, tablets, smartphones) die toegang hebben tot de GUI van een NAS of tot vertrouwelijke gegevens op die NAS, zouden beveiligd moeten zijn tegen Meltdown en Spectre. Voor een apparaat dat wordt getroffen door Meltdown of Spectre, geldt dat de bestanden waar het apparaat toegang toe heeft, gevaar lopen.

## 5.2 Coblin bNAS Pro

Voor de Coblin bNAS Pro is een BIOS upgrade beschikbaar; zie ook par 3.1. Daarnaast is een software upgrade van versie 9 naar versie 11 beschikbaar. Zie voor de BIOS upgrade ook par 4.2.

## 5.3 Netgear NAS systemen

Netgear werkt aan nieuwe firmware voor zijn NAS systemen.

# 6. Maatregelen voor de bSafe firewall

## 6.1 Beveilig apparaten die toegang hebben

Apparaten (PC's, tablets, smartphones) die toegang hebben tot de GUI van de bSafe firewall, zouden beveiligd moeten zijn tegen Meltdown en Spectre.

## 6.2 Jonger dan 5 jaar

Informeer bij bSafe firewalls jonger dan 5 jaar bij Coblin of er een BIOS upgrade beschikbaar is. Wanneer die beschikbaar is, adviseren wij om deze te laten uitvoeren. Zie hiervoor ook par 4.2.

## 6.3 Ouder dan 5 jaar

Voor deze systemen komt waarschijnlijk geen BIOS upgrade beschikbaar. Hoewel de risico's waarschijnlijk beperkt zijn wanneer de richtlijn uit par 6.1 wordt overgenomen, is er sprake van een beveiligingsrisico. Vervanging is dan ook het overwegen waard.