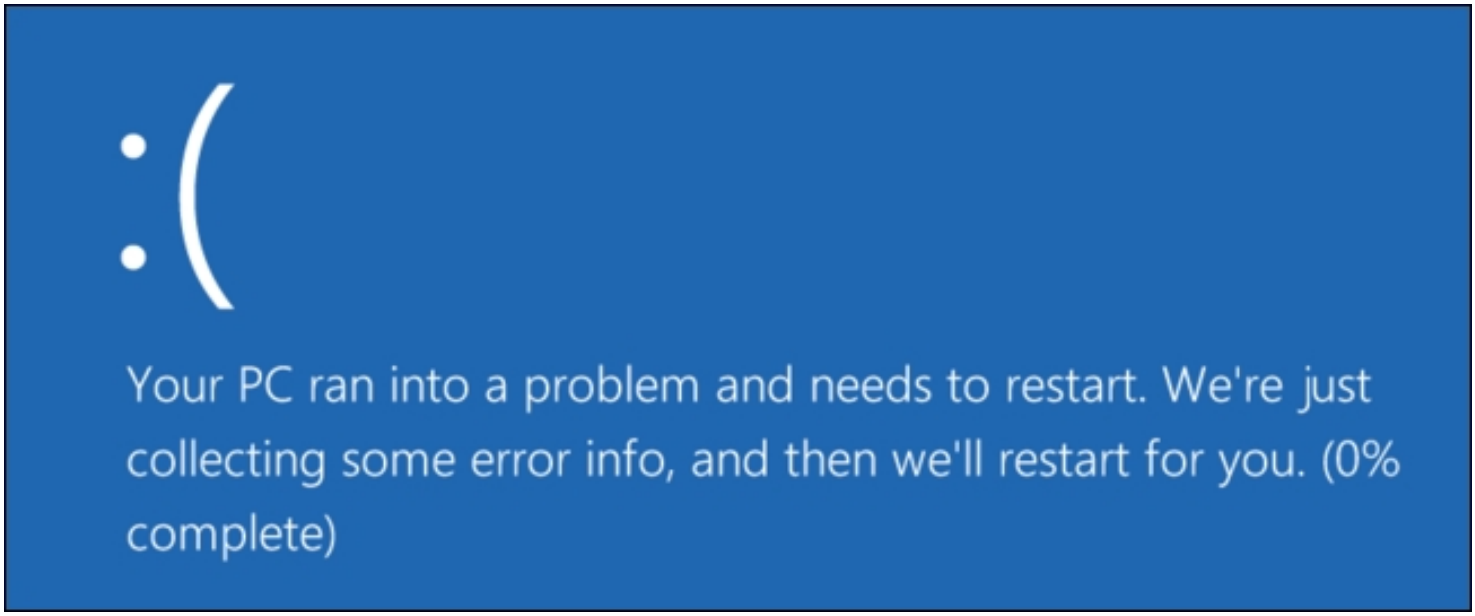

CVE-2020-16898 | Windows 10 Patch Tuesday

Correction et QuickWin d'une faille de sécurité critique type "Ping of Death"

Une nouvelle faille d'exécution de code à distance critique : CVE-2020-16898, qui exploite une faille dans la pile TCP / IP de Windows lorsqu'il ne gère pas correctement les paquets d'annonce de routeur ICMPv6.

Comme Microsoft l'écrit:

"Il existe une vulnérabilité d'exécution de code à distance lorsque la pile TCP/IP Windows ne gère pas correctement les paquets d'annonce de routeur ICMPv6.

Un attaquant qui parviendrait à exploiter cette vulnérabilité pourrait avoir la possibilité d'exécuter du code sur le serveur ou le client cible.

Pour exploiter cette vulnérabilité, un attaquant doit envoyer des paquets d'annonce de routeur ICMPv6 spécialement conçus à un ordinateur Windows distant."

Maintenant qu'un correctif est disponible, il doit être appliqué de toute urgence, puisque la faille a un score CVSS de **9.8** et a été classé dans la catégorie «exploitation plus probable» et plus important est «Wormable».

Il existe également une faille de déni de service (CVE-2020-16899) dans la pile

Windows TCP/IP, où un traitement incorrect des paquets d'annonce de routeur ICMPv6 permettrait à un attaquant de faire cesser de répondre un système cible.

«tout de même une bonne nouvelle c'est que l'équipe de sécurité interne de Microsoft a découvert les vulnérabilités, ce qui signifie que le code PoC n'apparaîtra probablement pas tant qu'on ne procédera pas à l'ingénierie inverse du correctif»

Les Patchs c'est par là => Portail MS

Sinon en attendant ci-dessous un petit QuickWin / Workaround en Powershell on sait jamais ça peut aider:

```
$interfaces = (Get-NetIPInterface | where {$_.AddressFamily -eq "IPv6"}).ifIndex

foreach ($interface in $interfaces)
{

  netsh int ipv6 set int $interface rabaseddnsconfig=disabled

}
```