Falha grave no Bluetooth afeta smartphones e computadores

Date : 13 de Setembro de 2017

O Bluetooth, quando foi lançado, veio abrir a porta a todo um conjunto novo de equipamentos, que comunicam sem fios e a curta distância. Todos os vêem como algo essencial e que não representa qualquer perigo de segurança para o utilizador.

A verdade é ligeiramente diferente e uma nova descoberta veio mostrar uma vulnerabilidade grave, que o deixa exposto a qualquer ataque, com danos nos equipamentos vulneráveis.

A falha foi descoberta pela equipa da Armis e, segundo o que foi descrito, afeta um vasto leque de equipamentos, desde os portáteis com Windows ou Linux, até aos smartphones com Android ou iOS. A empresa revelou também que existem vários vetores de ataque e que por isso esta é uma falha simples de explorar.

BlueBorne: um problema grave no Bluetooth

Na verdade, o BlueBorne, nome dado a esta falha, não necessita que exista qualquer ligação pré-estabelecida e nem sequer que o utilizador autorize qualquer permissão especial nas aplicações.

O ataque funciona através da exploração de falhas no protocolo de comunicação usado pelo Bluetooth. Permite a injeção de código malicioso e, graças às permissões elevadas que os dispositivos Bluetooth têm nos sistemas, o ataque decorre deforma completamente silenciosa, permitindo depois o controlo da máquina.

https://youtu.be/LLNtZKpL0P8

A forma de operar do BlueBorne é semelhante à que era usada na falha nos chipset Wi-Fi da Broadcom, que afetava o iPhone e muitos dispositivos Android.

As soluções para o problema do Bluetooth

Uma vez que a Armis já reportou este problema em abril deste ano, várias marcas já conseguiram resolver o problema. No caso dos produtos da Apple, a marca resolveu a falha com o lançamento da versão 10 do iOS. Apenas as versões anteriores estão vulneráveis.

Também a Microsoft lançou hoje um patch para todos os seus sistemas operativos para resolver de forma definitiva o BlueBorne. Também no Linux há já várias soluções lançadas, na forma de atualizações.

O eterno problema do Android

O caso do Android é mais grave. Mais uma vez, e fruto da fragmentação, muitos são os dispositivos expostos ao problema. A Google, no âmbito do seu programa de atualizações de segurança já lançou uma correção, quer para o Android Nougat (7.0) como para o Marshmallow (6.0). Esta foi incluída na atualização de setembro.

Claro que isto vai deixar de forma muitos milhares de equipamentos, que não vão nunca receber qualquer atualização para resolver o BlueBorne, ou outras falhas anteriores.

O BlueBorne, dada a sua multiplicidade de vetores de ataque e a simplicidade de utilização, é uma falha grave e perigosa. A solução passa por ter o Bluetooth desligado, uma vez que basta a aproximação de um dispositivo infetado para que o ataque se dê, sem que sequer o utilizador dê por isso.