

Mais duas falhas no Windows 10

Esta é a terceira falha que aparece no site. O que está acontecendo com o Windows. Isto é natural, pois quanto maior o uso do mesmo mais erros aparecem. Se não tivesse nenhum erro é que era de se estranhar. O sistema de maior longevidade foi o Windows 95 (1995) e durante toda sua vida teve vários upgrades. Isto ainda acontece com o Windows 7. Se não aparecer algum substituto os "ups" vão continuar.

Google divulga mais uma falha no Windows 10 que ainda não foi corrigida¹



O Google divulgou mais uma falha de segurança antes da Microsoft soltar uma correção para ela. Dias depois de revelar um erro no navegador Edge, agora o Google detalhou um bug de segurança que atinge o Windows 10.

A divulgação da falha acontece 90 dias após o Google notificar a Microsoft sobre a existência dela. Em novembro, pesquisadores de segurança do Google descobriram um erro que permite a um usuário normal ganhar acesso de administrador de sistema. Até agora, a Microsoft não soltou nenhum patch para corrigir o erro.

Ao ser alertada, a Microsoft classificou o erro como "importante", mas não "crítico", já que ele não pode ser explorado remotamente. Os pesquisadores do Google acreditam que, para a falha ser usada sem acesso direto ao computador, os hackers precisariam combiná-la com a execução remota de um código.

Ainda não está claro se a Microsoft pretende corrigir o erro. A empresa ainda não soltou um patch para a falha no Edge divulgada no começo da semana pelo Google. Ao Neowin, o Google [disse](#) que o fato das duas vulnerabilidades terem sido divulgadas tão próximas foi apenas coincidência, e não algo planejado.

¹ Redação Olhar Digital 21/02/2018 Google Microsoft Segurança

Segunda Falha no Windows 10 impedia antivírus de analisar códigos de alguns programas²



Uma ameaça poderia ter dado muita dor de cabeça à Microsoft. Foi descoberta uma vulnerabilidade no Windows 10 que impedia que algumas linhas de código fossem analisadas pelo antivírus em condições específicas, o que permitiria que malwares se instalassem no computador sem serem notados.

A vulnerabilidade reside no AMSI (sigla para Interface de Escaneamento Antimalware), um novo recurso implementado no Windows 10 que simplifica a análise de arquivos e programas através de código malicioso criando um canal entre o sistema operacional e seus aplicativos e o software de antivírus de sua preferência.

O que acontecia é que o AMSI se tornou incapaz de analisar o código de arquivos que contassem com um caractere nulo. Isso significa que todas as linhas de código após o tal caractere deixavam de ser analisadas. Assim, um cibercriminoso ciente desta falha precisaria apenas incluir o código após o símbolo que faz o AMSI parar de funcionar para passar indetectado.

Satoshi Tanda, o pesquisador responsável por encontrar a falha, que o problema afetava especificamente conteúdo PowerShell. Diante do caractere nulo, o sistema entendia que se tratava do final do código, encerrando o escaneamento.

Felizmente, Tanda alertou a Microsoft e a falha já foi corrigida na última "Patch Tuesday", termo que se refere normalmente à segunda terça-feira do mês, quando a empresa libera atualizações regulares de segurança para seus produtos. Vale a pena atualizar seu Windows para se manter seguro.

² Renato Santino 20/02/2018 Microsoft Segurança Windows