Cách bảo vệ máy tính trước lỗ hổng bảo mật Foreshadow

Foreshadow là gì?

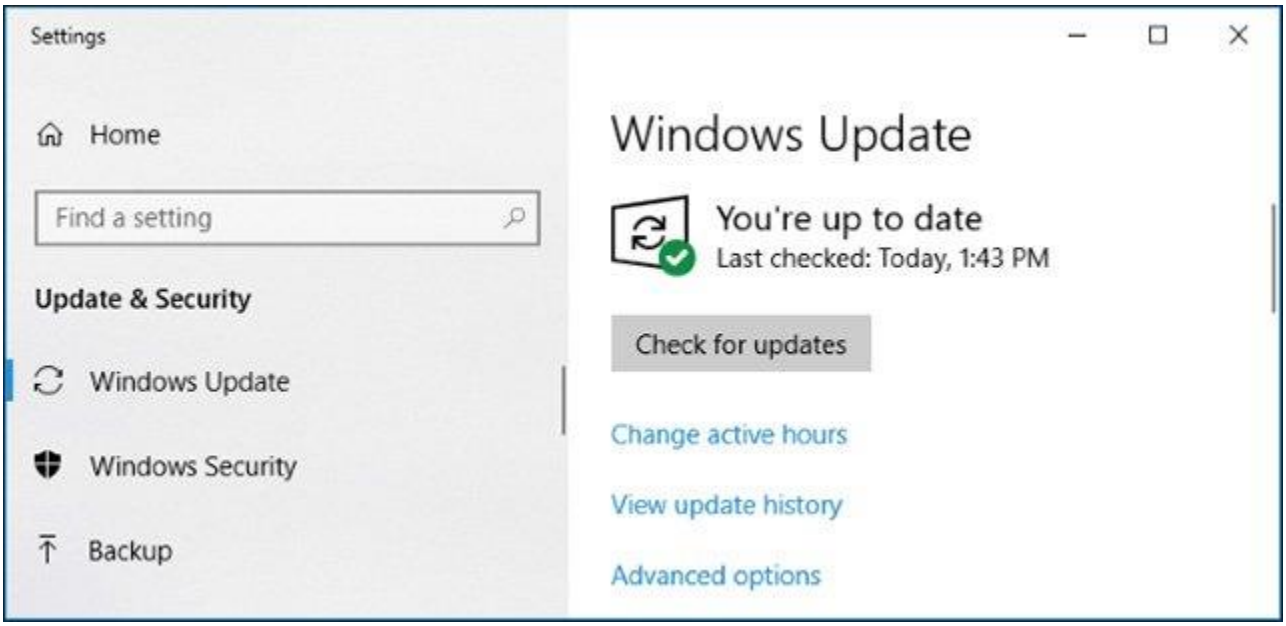
Foreshadow, hay còn được gọi là L1 Terminal Fault, là một lỗi bảo mật ảnh hưởng tới một trong các phần tử bảo mật của chip Intel - Software Guard Extensions (hay SGX).. Nó cho phép phần mềm độc hại xâm nhập vào các khu vực an toàn mà ngay cả những lỗ hổng bảo mật trước đây của Spectre và Meltdown cũng không thể phá vỡ.

Cụ thể, Foreshadow tấn công tính năng tiện ích bảo vệ phần mềm (SGX) của Intel. Tính năng này được tích hợp vào các chip Intel nhằm cho phép các chương trình tạo "các vùng" an toàn mà ngay cả các chương trình khác trên máy tính cũng không thể truy cập được. Ngoài ra, theo lý thuyết, ngay cả khi phần mềm độc hại xâm nhập vào máy tính, nó cũng không thể truy cập vào những vùng an toàn này. Khi các lỗi bảo mật Spectre và Meltdown được công bố, các nhà nghiên cứu bảo mật phát hiện ra rằng bộ nhớ được bảo vệ bởi SGX hầu như không bị tấn công bởi Spectre và Meltdown.

Foreshadow có 2 phiên bản: kiểu tấn công ban đầu là lấy dữ liệu từ vùng an toàn của SGX và thứ hai là Foreshadow NG (Next Generation) dùng để lấy thông tin

nằm trong bộ nhớ đệm L1. NG ảnh hưởng tới cả máy ảo, bộ nhớ nhân OS, bộ nhớ quản lý hệ thống, có khả năng đe dọa toàn bộ kiến trúc nền tảng đám mây.

Cách bảo vệ PC của bạn trước Foreshadow



Lưu ý rằng chỉ những máy tính sử dụng chip Intel mới dễ bị Foreshadow tấn công. Các chip AMD rất hiếm khi mắc phải lỗi bảo mật này.

Theo lời khuyên bảo mật chính thức từ Microsoft, hầu hết các PC chạy Windows chỉ cần được cập nhật hệ điều hành là có thể tự bảo vệ mình khỏi Foreshadow. Chỉ cần chạy Windows Update để cài đặt các bản vá mới nhất. Microsoft cũng cho biết họ không nhận thấy bất kỳ ảnh hưởng nào liên quan đến hiệu suất của máy sau khi cài đặt các bản vá này.

Một số PC cũng có thể sẽ phải cần đến các vi mã mới từ Intel để tự bảo vệ mình. Intel cho biết đây là những bản cập nhật các vi mã giống nhau đã được phát hành đầu năm nay. Bạn hoàn toàn có thể có được bản cập nhật firmware mới, bằng cách cài đặt bản cập nhật UEFI hoặc BIOS mới nhất từ hoặc nhà sản xuất PC hoặc bo mạch chủ của bạn. Ngoài ra, cũng có thể cài đặt bản cập nhật các vi mã trực tiếp từ Microsoft.

Những lưu ý đối với các nhà quản trị hệ thống

Đối với các PC đang chạy phần mềm hypervisor cho các máy ảo (ví dụ, Hyper-V) phần mềm hypervisor đó cũng sẽ cần phải được cập nhật phiên bản mới nhất. Ví dụ, ngoài bản cập nhật mà Microsoft dành cho Hyper-V, VMWare cũng đã phát hành bản cập nhật cho phần mềm máy ảo này của họ.

Các hệ thống sử dụng Hyper-V hoặc các nền tảng bảo mật dựa trên ảo hóa khác cũng sẽ cần những thay đổi mạnh mẽ hơn. Bao gồm việc vô hiệu các siêu phân luồng, điều này sẽ làm máy tính chậm đi, và tất nhiên hầu hết mọi người sẽ không cần phải thực hiện thao tác này, nhưng đối với các quản trị viên Windows Server đang chạy Hyper-V trên CPU của Intel, họ sẽ cần phải cân nhắc một cách nghiêm túc về việc vô hiệu hóa siêu phân luồng trong BIOS của hệ thống nhằm giữ cho máy ảo của họ được an toàn.

Các nhà cung cấp tiện ích đám mây như Microsoft Azure và Amazon Web Services cũng đang tích cực chạy các bản vá cho hệ thống của mình để tránh việc các máy ảo trên các hệ thống chia sẻ dữ liệu này bị tấn công.

Các hệ điều hành khác cũng cần phải được cập nhật những bản vá bảo mật mới. Ví dụ, Ubuntu đã phát hành bản cập nhật mới để bảo vệ các máy Linux trước các cuộc tấn công này. Trong khi Apple vẫn chưa đưa ra bất cứ động thái chính thức nào.

Sau khi xác định và phân tích các số liệu CVE các nhà bảo mật đã xác định được các lỗi như sau: CVE-2018-3615 để tấn công vào Intel SGX, CVE-2018-3620 tấn công vào hệ điều hành và chế độ quản lý hệ thống và CVE-2018-3646 để tấn công vào việc quản lý các máy ảo.

Trong một bài đăng trên blog, Intel cho biết họ đang tích cực làm việc để đưa ra các giải pháp tốt hơn cũng như cải thiện hiệu suất đồng thời đẩy mạnh việc chặn các ảnh hưởng đến từ L1TF. Các giải pháp này sẽ chỉ được áp dụng khi cần thiết. Intel cho biết các vi mã cho CPU được hãng phát hành trước đó đã cung cấp tính năng này cho một số đối tác và hiệu quả của nó vẫn đang được đánh giá.

Cuối cùng, Intel lưu ý rằng các vấn đề về L1TF cũng sẽ được hãng giải quyết bằng những thay đổi được thực hiện đối với phần cứng. Nói cách khác, các CPU của Intel trong tương lai sẽ mang trong mình các cải tiến về phần cứng để nâng cao hiệu quả trong việc chống lại Spectre, Meltdown, Foreshadow và các cuộc tấn công tương tự khác cũng như giảm thiểu các thiệt hại đến mức tối thiểu.