**Cảnh báo lỗ hổng nghiêm trọng mới trong dịch vụ Remote Desktop ảnh hưởng tới nhiều phiên bản hệ điều hành Windows**

**Mã lỗi quốc tế :** CVE-2019-1181; CVE-2019-1182, CVE-2019-1222, CVE-2019-1223, CVE-2019-1224, CVE-2019-1225, CVE-2019-1226.

**Các phiên bản hệ điều hành ảnh hưởng:** Windows 7 SP1, Windows 8.1, Windows 10, và các phiên bản Windows Server 2008 R2 SP1 trở lên. Chi tiết có thể xem thông tin từng lỗ hổng.

**Thông tin về lỗ hổng**

CVE-2019-1181 và CVE-2019-1182 là 02 lỗ hổng, điểm yếu an toàn thông tin mới được công bố, tồn tại trong dịch vụ truy cập máy tính từ xa (Remote Desktop Services) của Hệ điều hành Windows. 02 lỗ hổng này cho phép đối tượng tấn công thực thi mã từ xa để cài cắm mã độc và kiểm soát hệ thống mục tiêu. Đặc biệt khi đã có 1 máy trong mạng bị cài cắm mã độc thì các máy khác trong cùng vùng mạng cũng có thể bị khai thác và cài cắm mã độc một cách tự động.

Theo thống kê sơ bộ, Cục An toàn thông tin nhận thấy hiện nay có hơn **22.000** máy tính ở Việt Nam đang mở cổng RDP - Remote Desktop Protocol (TCP 3389) trên Internet, nếu các máy tính này chưa cập nhật bản vá thì sẽ trở thành mục tiêu khai thác đầu tiên và lây nhiễm sang các máy khác trong cùng vùng mạng.

Các lỗ hổng này Microsoft đã phát hành bản vá ngày 13/8/2019. Ngoài ra còn một số lỗ hổng khác trên dịch vụ Remote Desktop (CVE-2019-1222, CVE-2019-1223, CVE-2019-1224, CVE-2019-1225, CVE-2019-1226) cũng cho phép thực thi mã lệnh đã được Microsoft công bố và phát hành bản vá.

**Khuyến nghị**

(1) Cán bộ quản trị hệ thống của các cơ quan, tổ chức cần rà soát toàn bộ máy tính, máy chủ của đơn vị mình. Tổng hợp danh sách thiết bị bị ảnh hưởng (tham khảo Thông tin chi tiết các phiên bản bị ảnh hưởng *tại Phụ lục* kèm theo) để cập nhật các bản vá lỗi cho từng sản phẩm mà Microsoft đã phát hành. Khuyến nghị sử dụng chức năng cập nhật bản vá tự động của Windows, và khởi động lại máy sau khi đã cập nhật bản vá.

(2) Hạn chế tối đa việc mở cổng dịch vụ Remote Desktop. Trong trường hợp cần sử dụng phải thiết lập các chính sách bảo mật như: sử dụng VPN, giới hạn IP truy cập, tài khoản được phép truy cập, chính sách mật khẩu mạnh (mật khẩu có tối thiểu 8 ký tự, có đầy đủ chữ hoa, chữ thường, số và ký tự đặc biệt) v.v… Tham khảo hướng dẫn chi tiết do Trung tâm giám sát an toàn không gian mạng quốc gia (NCSC) đã phát hành *(file hướng dẫn kèm theo)*.

(3) Định kỳ sao lưu dữ liệu quan trọng trên máy chủ;

(4) Theo dõi, giám sát hệ thống để phát hiện sớm, kịp thời phản ứng các hành vi dò quét/tấn công mạng.

(5) Thông tin chi tiết về từng lỗ hổng và bản vá cập nhật tại:

- https://portal.msrc.microsoft.com/en-us/security-guidance

- https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1182

- https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1181

- https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2019-1222

- https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2019-1223

- https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2019-1224

- https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2019-1225

- https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2019-1226

Trong trường hợp cần thiết, có thể liên hệ Trung tâm Giám sát an toàn không gian mạng quốc gia thuộc Cục ATTT, số điện thoại: 024.3209.1616, thư điện tử ais@mic.gov.vn để được hỗ trợ kịp thời./.

**Phụ lục**

**Chi tiết các phiên bản hệ điều hành bị ảnh hưởng**

*(CVE-2019-1181, CVE-2019-1182)*

|  |
| --- |
| **Hệ điều hành bị ảnh hưởng** |
| Windows 10 for 32-bit Systems |
| Windows 10 for x64-based Systems |
| Windows 10 Version 1607 for 32-bit Systems |
| Windows 10 Version 1607 for x64-based Systems |
| Windows 10 Version 1703 for 32-bit Systems |
| Windows 10 Version 1703 for x64-based Systems |
| Windows 10 Version 1709 for 32-bit Systems |
| Windows 10 Version 1709 for 64-based Systems |
| Windows 10 Version 1709 for ARM64-based Systems |
| Windows 10 Version 1803 for 32-bit Systems |
| Windows 10 Version 1803 for ARM64-based Systems |
| Windows 10 Version 1803 for x64-based Systems |
| Windows 10 Version 1809 for 32-bit Systems |
| Windows 10 Version 1809 for ARM64-based Systems |
| Windows 10 Version 1809 for x64-based Systems |
| Windows 10 Version 1903 for 32-bit Systems |
| Windows 10 Version 1903 for ARM64-based Systems |
| Windows 10 Version 1903 for x64-based Systems |
| Windows 7 for 32-bit Systems Service Pack 1 |
|
| Windows 7 for x64-based Systems Service Pack 1 |
|
| Windows 8.1 for 32-bit systems |
|
| Windows 8.1 for x64-based systems |
|
| Windows RT 8.1 |
| Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1 |
|
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 |
|
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) |
|
| Windows Server 2012 |
| Windows Server 2012 (Server Core installation) |
|
| Windows Server 2012 R2 |
|
| Windows Server 2012 R2 (Server Core installation) |
|
| Windows Server 2016 |
| Windows Server 2016 (Server Core installation) |
| Windows Server 2019 |
| Windows Server 2019 (Server Core installation) |
| Windows Server, version 1803 (Server Core Installation) |
| Windows Server, version 1903 (Server Core installation) |