[추가]윈도우 **RDP** 원격코드실행 취약점 보안 업데이트 권고

글쓴이: hwkadmin-power. / 작성시간: 금, 05/17/2019 - 16:41

[추가] 윈도우 RDP 원격코드실행 취약점 보안 업데이트 권고

- 개요
  - 최근 윈도우 RDP 원격코드실행 취약점(CVE-2019-0708)을 악용할 수 있는 개념증명코드(Proof of concept code, PoC)가 인터넷상에 공개되어 윈도우 사용자의 보안 강화 필요

    ※ 개념증명코드 : 취약점을 증명/검증할 수 있는 프로그램 또는 소스코드

    ※ 기술지원이 종료된 Windows XP, Windows Server 2003까지 보안업데이트 제공
- 주요 내용
  - 윈도우 RDP 원격코드실행 취약점(CVE-2019-0708)를 악용코드가 인터넷상에 공개되어 서비스 거부 공격 및 랜섬웨어 감염 등에 악용될 수 있음
  - 윈도우 원격 데스크톱 프로토콜(Remote Desktop Protocol, RDP) 서비스(기본포트:3389)가 실행되고 있고 최신 보안
    업데이트가 적용되어 있지 않을 경우 공격 위험에 노출
  - 취약점에 영향받는 윈도우 제품을 이용하는 각 기관, 기업 및 일반 사용자는 해당 취약점에 노출되지 않도록 보안 업데이트 적용 및 RDP 보안 강화 필요
- **취약점에 영향 받는 윈도우 제품**

  - Windows XP SP3 x86

  - Windows XP Professional x64 Edition SP2

  - Windows XP Embedded SP3 x86

  - Windows Server 2003 SP2 x86

  - Windows Server 2003 x64 Edition SP2

  - Windows 7 for 32-bit Systems Service Pack 1

  - Windows 7 for x64-based Systems Service Pack 1

  - Windows Server 2008 for 32-bit Systems Service Pack 2

  - Windows Server 2008 for x64-based Systems Service Pack 2

  - Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1

  - Windows Server 2008 R2 for x64-based Systems Service Pack 1

- 대응 방안
  - 윈도우 OS에 대한 최신 보안 업데이트 적용(KISA 보안공지 1193번 참고)
  - RDP 사용하지 않을 시, 서비스 비활성화
  - RDP 사용이 불가피할 시, 인가된 관리자 IP주소에서만 윈도우 RDP를 접근할 수 있도록 방화벽 등을 통한 접근 통제 강화 및 기본 포트 번호(3389)를 다른 포트로 변경하여 사용
  - 백신 설치 및 정기적으로 최신 업데이트 수행
- 문의사항
  - 마이크로소프트 코리아 고객센터: 1577-9700
  - 한국인터넷진흥원 인터넷침해대응센터: 국번없이 118
- **[업데이트 다운로드 웹사이트]**
  - [1] https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2... [1]
  - [2] https://support.microsoft.com/en-us/help/4500705/customer-guidance-for-c... [2]

호스트웨이는 앞으로 더욱더 나은 서비스를 제공하기 위해 노력하겠습니다.
Global IT Service Partner HOSTWAY

date:

Source URL (retrieved on *10/17/2019 - 15:31*):
http://www.hostway.co.kr/news/%EC%B6%94%EA%B0%80%EC%9C%88%EB%8F%84%EC%9A%B0-rdp-%EC%9B%90%EA%B2%A9%EC%BD%94%EB%93%9C%EC%8B%A4%ED%96%89-%EC%B7%A8%EC%95%BD%EC%A0%90-%EB%B3%B4%EC%95%88-%EC%97%85%EB%8D%B0%EC%9D%B4%ED%8A%B8-%EA%B6%8C%EA%B3%A0

링크:
[1] https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0708
[2] https://support.microsoft.com/en-us/help/4500705/customer-guidance-for-cve-2019-0708