

Sana Security Advisory

August 9, 2005

Threat Summary

A vulnerability has been reported in the Microsoft Plug-and-Play service, 'services.exe', that may allow attackers to DoS or compromise vulnerable systems.

Affected Systems

- Microsoft Windows 2000 Advanced Server
- Microsoft Windows 2000 Datacenter Server
- Microsoft Windows 2000 Server
- Microsoft Windows Server 2003 Datacenter Edition
- Microsoft Windows Server 2003 Enterprise Edition
- Microsoft Windows Server 2003 Standard Edition
- Microsoft Windows Server 2003 Web Edition
- Microsoft Windows XP Professional

Mitigation

Can Primary Response protect me?

Yes, Primary Response can protect against exploits targeting this vulnerability.

Does an out of the box configuration protect me?

Yes. By default Primary Response versions 2.3, 3.0, and 3.1 protect 'services.exe' from stack, static, and heap overflows. On clients, Primary Response versions 3.0 and 3.1 protect against return to libc attacks as well.

Are there additional actions I must take to become protected?

Sana Security recommends applying the latest patches from Microsoft. Those can be found at: <http://www.microsoft.com/technet/security/Bulletin/MS05-039.mspx>

Threat Vectors

This attack works by exploiting an unchecked stack buffer. This unchecked buffer could allow an attacker to run arbitrary code on the victim machine.