

By Deb Shinder, MCSE, MVP

Service hardening is one of many new security mechanisms in Windows Vista and the next generation of Windows server, currently known as Longhorn Server. Because it's not always desirable or possible to disable Windows services that provide attackers with an exploitable point of attack, the new operating systems include features that make it more difficult for service exploits to do damage.

Here are a few facts you should know about service hardening.

1 SCM manages services

Windows services are programs that are managed by the Service Control Manager (SCM), which maintains a database of installed services and manages each service's state. Usually services start automatically when Windows boots and run continuously, making them always available and thus attractive to attackers.

2 Higher privileges = greater exposure

In previous Windows operating systems, most services ran under the LocalSystem account, which has a high level of privileges. That meant that if the service were compromised, attackers could do major damage because they would have access to almost everything.

3 Vista and Longhorn Server run services with lowest possible privileges

In Vista and Longhorn, many of the services that used to run under LocalSystem now run under the NetworkService or LocalService accounts, which have a lower level of privileges. Services run with the lowest possible privileges. Any privileges that a service doesn't need are removed, which helps reduce the attack surface.

4 Vista protects services by using "isolation" techniques

Isolation techniques includes Session 0 isolation, which prevents user applications from running in Session 0 (the first session created when Windows starts up). Only services and other applications that are not associated with a user session can run there. This protects the services from the actions of other applications.

5 Vista assigns a Security Identifier (SID) to each service

Assigning an SID to each service allows services to be separated from one another and enables the operating system to apply the Windows access control model to restrict services' access to resources in the same way user and group accounts' access can be restricted.

6 In Vista, access control lists (ACLs) can now be applied to services

An ACL is a set of access control entries (ACEs). Every resource on the network has a security descriptor that contains the ACLs assigned to it. Permissions defining who or what can access that resource are stored in the ACL.

7 Vista allows the application of network firewall policies to services

The policy is linked to the service's SID. This allows you to control how the service is allowed to access the network and prevent it from using the network in ways it's not supposed to, such as sending outbound network traffic. The Vista Firewall is integrated with the service hardening feature.

8 Specific services can be restricted so that they can't make edits to the registry, write to system files, and so forth

If a service needs to perform those actions to function properly, it can be restricted so that it can write only to specific areas of the registry or a file system. Services can also be prevented from making changes to configuration settings and performing other actions that can be exploited by an attacker.

9 Each service is pre-assigned a service hardening profile

This profile defines what the service should and shouldn't be allowed to do. Based on this profile, the SCM assigns the services only the privileges they must have. This all happens transparently, with no configuration or administrative overhead required.

10 Service hardening does not prevent attackers from compromising services

The Windows Firewall and other protective layers are designed to prevent that. The purpose of service hardening is to reduce the level of damage that can be done if the service *does* become compromised. It provides inner layer protection in Vista's multilayered security strategy.



Debra Littlejohn Shinder is a technology consultant, trainer and writer who has authored a number of books on computer operating systems, networking, and security. These include *Scene of the Cybercrime: Computer Forensics Handbook*, published by Syngress, and *Computer Networking Essentials*, published by Cisco Press. She is co-author, with her husband, Dr. Thomas Shinder, of *Troubleshooting Windows 2000 TCP/IP*, the best-selling *Configuring ISA Server 2000*, and *ISA Server and Beyond*.

Additional resources

- TechRepublic's [Downloads RSS Feed](#) **XML**
- Sign up for TechRepublic's [Downloads Weekly Update](#) newsletter
- Sign up for our [Windows Vista Report newsletter](#)
- Check out all of TechRepublic's [free newsletters](#)
- ["Installing Windows Vista: The good, the bad, and the ugly"](#) (TechRepublic download)
- ["Get an in-depth look at Vista firewall's advanced configuration features"](#) (TechRepublic download)
- "Vista's Windows Meeting Space offers enhanced functionality for real-time collaboration"

Version history

Version: 1.0

Published: January 2, 2007

Tell us what you think

TechRepublic downloads are designed to help you get your job done as painlessly and effectively as possible. Because we're continually looking for ways to improve the usefulness of these tools, we need your feedback. Please take a minute to [drop us a line](#) and tell us how well this download worked for you and offer your suggestions for improvement.

Thanks!

—The TechRepublic Downloads Team