IOActive Security Advisory

Title	Microsoft Windows CryptoAPI X.509 Spoofing Vulnerability
Severity	Moderate
Release Date	10/13/09
VUPEN ID	VUPEN/ADV-2009-2891
CVE ID	CVE-2009-2510 – CVE-2009-2511
Remotely Exploitable	Yes
Locally Exploitable	Yes
Discovered by	Dan Kaminsky (IOActive) Ian Wright and Jean-Luc Giraud (Citrix)

Technical Description

Two vulnerabilities have been identified in Microsoft Windows that could be exploited by attackers to bypass security restrictions.

The first issue is due to the Windows CryptoAPI incorrectly parsing a null terminator as the end of any values identified by an Object Identifier (OID) when processing ASN.1 information from X.509 certificates. This could allow spoofing attacks.

The second vulnerability is caused by an integer overflow error in the Windows CryptoAPI when parsing ASN.1 object identifiers from X.509 certificates (such as Common Name), which could allow an attacker to generate a malicious certificate that would be parsed incorrectly by the Windows CryptoAPI, impersonating another user or system.

Affected Products

- Microsoft Windows 2000 Service Pack 4
- Microsoft Windows XP Service Pack 2
- Microsoft Windows XP Service Pack 3
- Microsoft Windows XP Professional x64 Edition Service Pack 2
- Microsoft Windows Server 2003 Service Pack 2
- Microsoft Windows Server 2003 x64 Edition Service Pack 2
- Microsoft Windows Server 2003 SP2 (Itanium)

- Microsoft Windows Vista
- Microsoft Windows Vista Service Pack 1
- Microsoft Windows Vista Service Pack 2
- Microsoft Windows Vista x64 Edition
- Microsoft Windows Vista x64 Edition Service Pack 1
- Microsoft Windows Vista x64 Edition Service Pack 2
- Microsoft Windows Server 2008 (32-bit)
- Microsoft Windows Server 2008 (32-bit) Service Pack 2
- Microsoft Windows Server 2008 (x64)
- Microsoft Windows Server 2008 (x64) Service Pack 2
- Microsoft Windows Server 2008 (Itanium)
- Microsoft Windows Server 2008 (Itanium) Service Pack 2
- Microsoft Windows Server 2008 R2 (x64)
- Microsoft Windows Server 2008 R2 (Itanium)
- Microsoft Windows 7 (32-bit)
- Microsoft Windows 7 (x64)

Solution

Apply patches available from Microsoft:

<http://www.microsoft.com/technet/security/bulletin/MS09-056.mspx>

References

<http://www.vupe.com/english/advisories/2009/2891>

<http://www.microsoft.com/technet/security/bulletin/MS09-056.mspx>