

# NOTA INFORMATIVA

---

Anno: 2011

---

Numero: 0015

---

Data: 20/06/2011

---

## Aggiornamenti Windows XP<sup>(R)</sup>

**Blocco della condivisione  
cartelle residenti su Server  
AIX nell'ambito della LAN  
aziendale**

---

Nella settimana dal **14 al 17 giugno 2011** sono stati distribuiti da Microsoft tramite **Windows Update<sup>(R)</sup>** una serie di aggiornamenti connessi alla sicurezza che in alcuni casi, su piattaforme **Windows XP<sup>(R)</sup>**, hanno prodotto il **blocco della connessione alle cartelle condivise** residenti sul Server AIX.

Il gruppo di aggiornamenti cui si fa riferimento è di seguito dettagliatamente indicato:

- Aggiornamento cumulativo per la protezione di Internet Explorer (2530548)
- Una vulnerabilità in Vector Markup Language può consentire l'esecuzione di codice in modalità remota (2544521)
- Una vulnerabilità presente nel client SMB può consentire l'esecuzione di codice in modalità remota (2536276)
- Le vulnerabilità nel Distributed File System potrebbero consentire l'esecuzione di codice in modalità remota (2535512)
- Una vulnerabilità in MHTML può consentire l'intercettazione di informazioni personali (2544893)
- Una vulnerabilità nell'automazione OLE può consentire l'esecuzione di codice in modalità remota (2476490)
- Una vulnerabilità nel driver di funzioni ausiliario può consentire l'acquisizione di privilegi più elevati (2503665)

Da una prima analisi l'aggiornamento responsabile del blocco sembra essere quello con rif. **2536276** che agendo su **SMB** (Server Message Block) con l'obiettivo di proteggere il PC dall'esecuzione remota di comandi **blocca anche** la connessione in rete locale a propri server o ad altri PC per la **condivisione delle cartelle**.

Questa deduzione deriva anche dal fatto che nella documentazione di accompagnamento dell'aggiornamento (Bollettino Microsoft sulla sicurezza MS11-043) quale soluzione alternativa all'installazione si suggerisce la **chiusura** verso il mondo esterno delle porte **TPC/UDP 139** (NetBIOS Session Service) e **TCP/UDP 445** (Microsoft-DS Active Directory, Windows shares).

La prima delle due (139) è quella normalmente utilizzata sulla LAN aziendale per condividere le cartelle residenti su server "non Windows", mentre la seconda (445) è utilizzata per la condivisione delle cartelle tra PC in ambiente Windows.

Per risolvere il problema sorto sono possibili due soluzioni:

1. **disinstallare** l'aggiornamento con il codice di riferimento indicato;
2. **intervenire sulle predisposizioni** introdotte dall'aggiornamento al fine di tenere aperte le porte TCP/UDP 139 e 445 sulla LAN aziendale.  
Qualora si optasse per questa soluzione è ovviamente consigliato rivolgersi a personale esperto nella gestione del firewall installato sul PC.

I dettagli completi dell'aggiornamento sono reperibili alla pagina:

<http://www.microsoft.com/italy/technet/security/bulletin/default.mspx>

attraverso il link:

### **Bollettino Microsoft sulla sicurezza MS11-043 - Critico**

**Non risultano**, al momento della stesura della presente Nota Informativa, problemi introdotti dall'equivalente aggiornamento (rif. **2536275**) in ambiente **Windows Vista<sup>(R)</sup>** e **Windows 7<sup>(R)</sup>**.



Il bollettino è anche scaricabile dal sito [www.adelsystems.it](http://www.adelsystems.it) alla pagina **NEWS => FAQ - Domande e Risposte Frequenti**.

=====  
Fine documento  
=====