relativo bollettino di sicurezza è MS15-011 / KB 3000483.
Questo meccanismo richiede sia l'installazione di un aggiornamento di sicurezza, sia l'applicazione di specifiche impostazioni di Group Policy su TUTTI i computer del dominio che devono essere necessariamente basati su Windows Vista / Windows Server 2008 o versioni successive.
L'aggiornamento di sicurezza comprende anche un nuovo template di Group Policy (NetworkProvider.admx/adml) che indirizza i parametri da impostare.
Una volta applicato l'aggiornamento e il template di Group Policy, l'impostazione minima per mitigare il rischio in oggetto è la seguente:

"Hardened UNC Paths" → ENABLED, impostato come segue:

*\NETLOGON RequireMutualAuthentication=1, RequireIntegrity=1

*\SYSVOL RequireMutualAuthentication=1, RequireIntegrity=1

5.3 Sicurezza del Web Browser

Di seguito viene fornita una vista delle principali minacce e delle relative contromisure da adottare.

5.3.1 Architettura

Architettura	
Minaccia	- Accesso non autorizzato al sistema. - Violazione della sicurezza, rispetto alle politiche di sicurezza dell'organizzazione. - Violazione di leggi, di regolamenti, di obblighi contrattuali.
Contromisure	- Utilizzare un sistema di protezione del perimetro (Firewall) in grado di effettuare Web Application Firewalling, posizionato tra la rete dei client e tutte le altre. - Installare un IDS (intrusion detection system) o IPS (intrusion prevention system) in grado di analizzare le richieste Web. - Impedire la manipolazione DNS: utilizzare DNS attendibile e protetto. - Bloccare i punti di accesso wireless e utilizzare un sistema di protezione come Wi-Fi Protected Access 2 e access point non vulnerabili (con firmware aggiornato) rispetto all'attacco KRACK precedentemente citato. **Nota Bene.** Si tenga presente che i dispositivi portatili personali possono eludere tali contromisure.

5.3.2 Hardening

Hardening del browser	
Minaccia	- Accesso non autorizzato al sistema. - Compromissione delle comunicazioni. - Furto di credenziali di autenticazione (es. keylogger). - Violazione della sicurezza, rispetto alle politiche di sicurezza dell'organizzazione. - Violazione di leggi, di regolamenti, di obblighi contrattuali.
Contromisure	- Utilizzare il browser con un account utente a bassi privilegi (ovvero senza privilegi di amministratore) in modo da limitare le possibilità di un attacco (security exploit) di compromettere l'intero sistema operativo. - Impostare il browser in modo da controllare la validità dei certificati presentati dai server, utilizzando le liste di revoca dei certificati (CRL), l'Online Certificate Status