

Atelier Sécurité / OSSIR



eEye® Digital Security

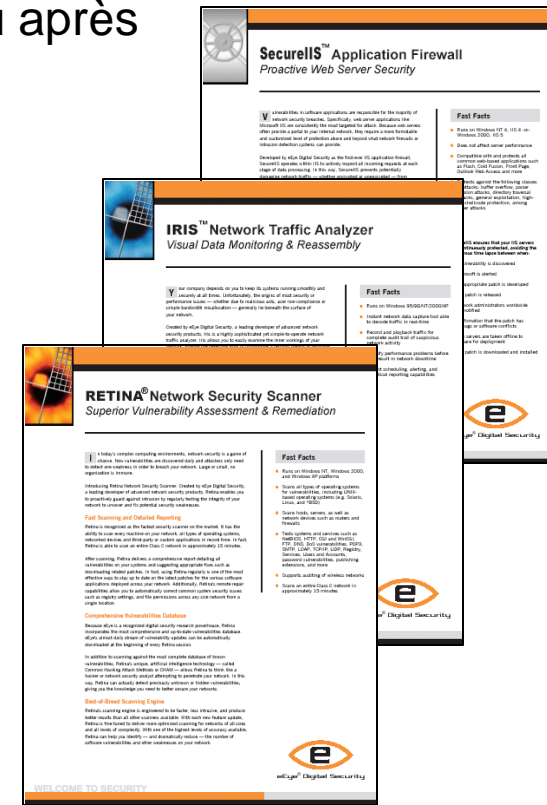
***Présentation Produits eEye
SecurellS
Retina***

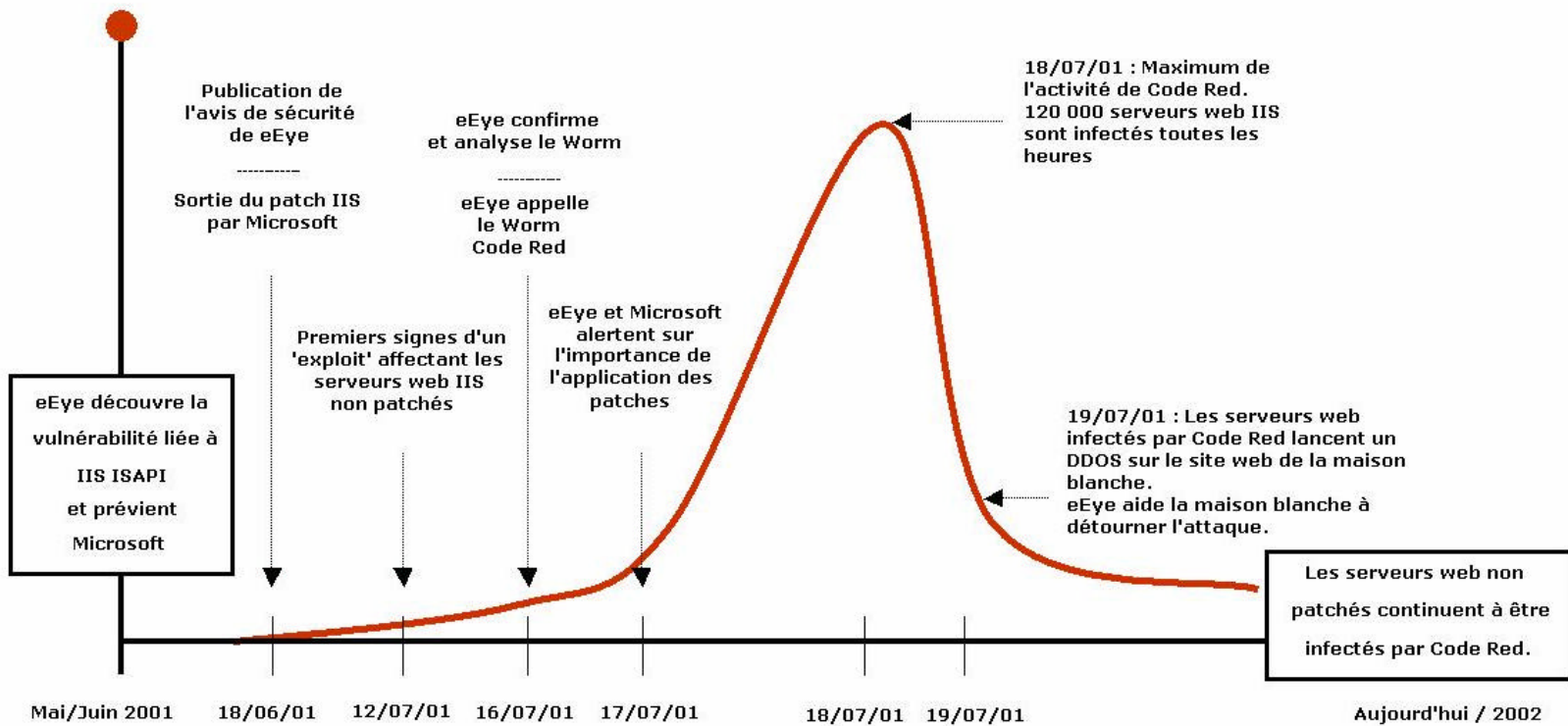
elorrain@eeye.com & broussel@eeye.com

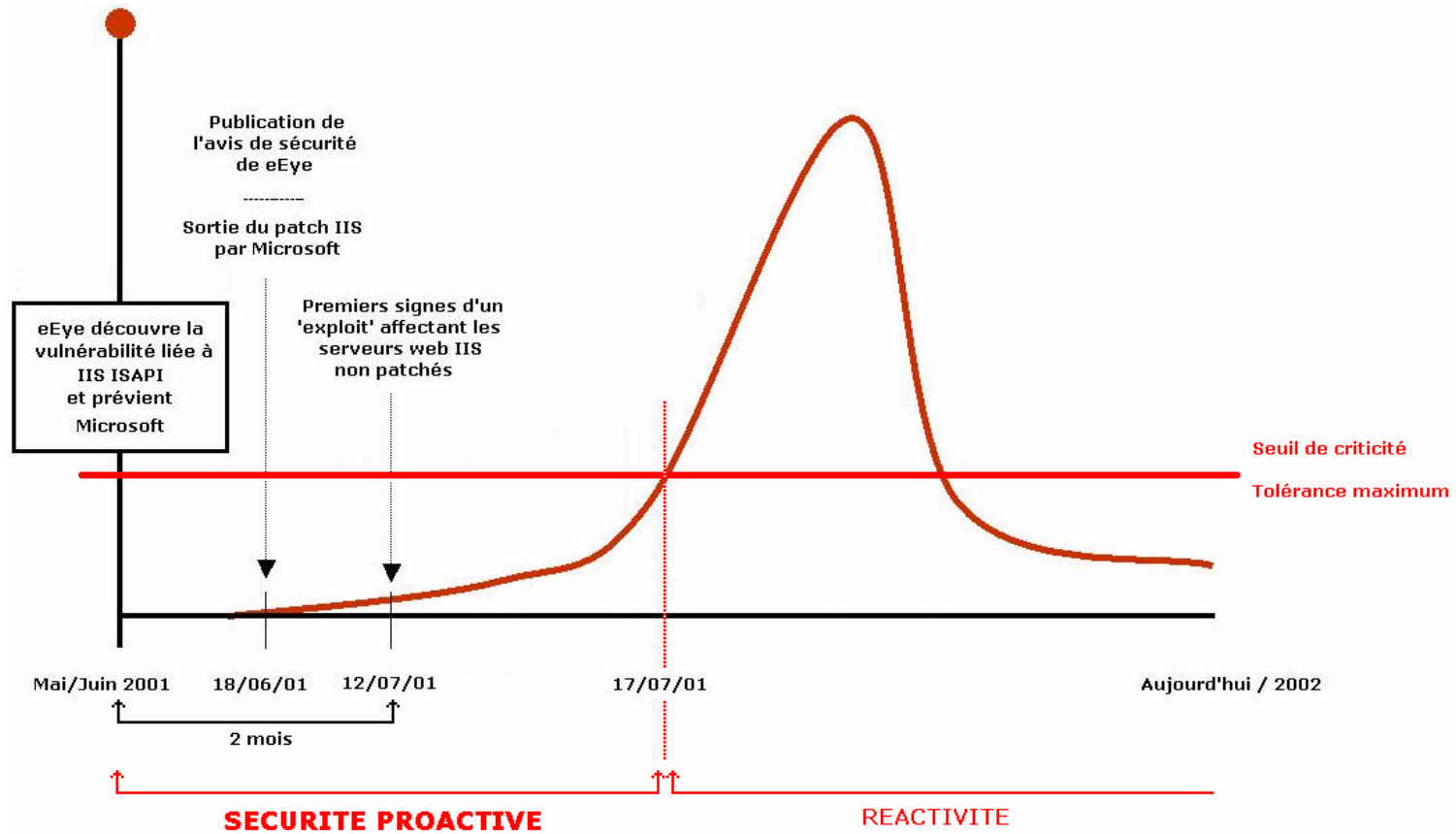
- **Qui sommes nous ?**
- **SecurellS – Protection Web**
- **Retina – Scanner de Sécurité**
- **Questions**

- **Créé en 1998**
- **Siège aux USA (CA) / Siège international à Genève**
- **Filiales à Londres et Paris**
 - Clients dans plus de 40 pays
 - Partenaires dans plus de 20 pays
- **Mission**
 - Développer des **logiciels** innovants dédiés à la **sécurité proactive**, destinés aux administrateurs réseaux et consultants. Ces produits complètent des outils comme les firewalls, les systèmes de détection d'intrusion ou les scanners de virus, pour obtenir une sécurité la plus complète possible.
- **Focus sur les vulnérabilités**
 - Le développement des produits eEye Digital Security repose sur la solide expérience de notre R&D. **eEye Digital Security** est reconnu comme étant **un des leaders dans la détection & évaluation de vulnérabilités**. (Découverte de la vulnérabilité utilisé par Code Red et de 90% des vulnérabilités de Microsoft IIS).

- **Produits dédiés à la sécurité proactive**
 - Se protéger AVANT l'attaque – non pas pendant ou après
 - CHAM (Common Hacking Attack Methods)
- **Conçus pour compléter les solutions existantes**
 - Firewalls
 - Intrusion Detection Systems (IDS)
 - Virus Scanners
- **Objectif : Simplicité**
 - Facile à installer, à mettre à jour, à utiliser
 - Fonctions de reporting personnalisable
 - Facilité pour mesurer le ROI (Time & Security)





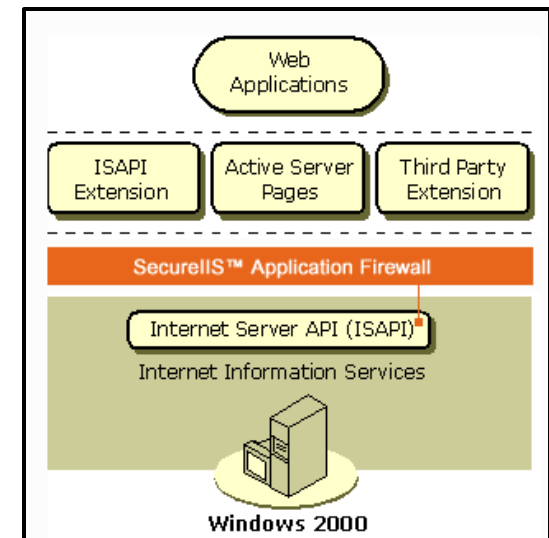


- **RETINA® Network Security Scanner**
Détection, évaluation et correction des vulnérabilités
 - Le plus Rapide et le plus Complet des Scanners
(Network World February 2002)
- **SecureIIS™ Web Server Protection**
La sécurité proactive de vos serveurs Web
 - Firewall Applicatif pour Microsoft IIS
- **IRIS™ Network Traffic Analyzer**
Surveillance et reconstitution visuelle du trafic réseau
 - Enregistre les Données transitant sur le Réseau et les restitue en Différé ou en Temps Réel
 - Met en évidence les Infractions de Sécurité



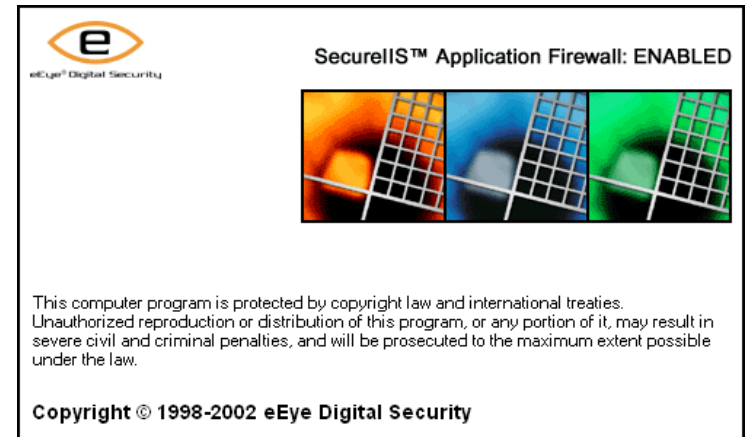


- Le premier Firewall applicatif dédié à IIS
- Le seul produit intégré à MS IIS en tant que filtre ISAPI qui protège le Web Server contre des classes entières d'attaques
- Gestion centralisée des règles
- Archivage des requêtes rejetées.
- Paramétrage global & dynamique
- Statistiques temps réel
- Protection non intrusive
- Protection des applications
- Protection des sessions SSL
- Exportation des logs
- Compatible avec les applications Web (Outlook Web Access, Front Page, ...)
- Monitoring du système de fichiers



SecurellS protège les Serveurs Web contre différents types d'attaques :

- **Dépassement de buffer**
- **Sortie du répertoire racine**
- **Exploits**
- **Protection contre les Shell Codes**
- **Vérification des RFC**
- **Vulnérabilités non connues**
- **Autres attaques...**



Plusieurs sites Web sur un même serveur peuvent être protégés

Type de classes d'attaques – Chaque onglet représente une catégorie d'attaque – chaque sous catégorie d'attaque est paramétrable

Paramètres par classe d'attaque

Chaque classe d'attaque est décrite en détails avec une aide pour la configuration

The screenshot shows the eEye Security Console interface. The main window is titled "Site Security" and displays a list of attack classes under the "Buffers" tab. The list includes various parameters such as "Maximum URL Length Allowed" (1024), "Maximum Query Length Allowed" (1024), "Maximum Post Query Length Allowed" (10000), and "Maximum Generic Query Variable Length Allowed" (128). A "Did you know..." section at the bottom provides additional information about the Beta version of SecureIIS 2.0.

Attack Class	Maximum Size
<input checked="" type="checkbox"/> Buffer Overflow	
<input checked="" type="checkbox"/> Maximum URL Length Allowed	1024
<input checked="" type="checkbox"/> Maximum Query Length Allowed	1024
<input checked="" type="checkbox"/> Maximum Post Query Length Allowed	10000
<input checked="" type="checkbox"/> Maximum Generic Query Variable Length Allowed	128
<input checked="" type="checkbox"/> Maximum Generic Query Data Length Allowed	512
<input checked="" type="checkbox"/> Maximum Generic Header Length Allowed	1024
<input type="checkbox"/> Maximum Accept Length Allowed	256
<input type="checkbox"/> Maximum Referer Length Allowed	256
<input type="checkbox"/> Maximum Accept-Language Length Allowed	256
<input type="checkbox"/> Maximum Accept-Encoding Length Allowed	256
<input type="checkbox"/> Maximum User-Agent Length Allowed	256
<input type="checkbox"/> Maximum Host Length Allowed	256
<input type="checkbox"/> Maximum Connection Length Allowed	256
<input type="checkbox"/> Maximum Cookie Length Allowed	256
<input type="checkbox"/> Maximum If-Modified-Since Length Allowed	256
<input type="checkbox"/> Maximum If-None-Match Length Allowed	256
<input type="checkbox"/> Maximum Authorization Length Allowed	256
<input checked="" type="checkbox"/> Maximum Transfer-Encoding Length Allowed	1

Buffer Overflows
Each variable is listed with a numeric entry specifying the maximum size of the buffer that your Web server will accept for that particular variable. This value can be increased or decreased according to your specific needs. If a client sends a variable value with a length greater than the limit specified by SecureIIS, the request will be denied and logged.
Caution: Setting size values too low may cause various features of your website to lose functionality. If this occurs, simply increase the value.

Did you know...
This is an **Beta** version of SecureIIS 2.0

SecureIIS

- Sécurité du site
- Surveillance des fichiers
- Statistiques du site

Journalisation

Options

Sécurité du site

DELATOURSOTWAR

- Tous les sites
- Default Web Site (1)

Mémoire tampons	Méthodes	Code de commande	Mots-clés	Protection
<input checked="" type="checkbox"/>	Débordement de la mémoire tampon		Taille maximale	
<input checked="" type="checkbox"/>	Longueur maximale d'URL autorisée		1024	
<input checked="" type="checkbox"/>	Longueur maximale de requête autorisée		1024	
<input type="checkbox"/>	Longueur maximale de requête POST autorisée		10000	
<input checked="" type="checkbox"/>	Longueur maximale de variable de requête générique autorisée		128	
<input checked="" type="checkbox"/>	Longueur maximale de donnée de requête générique autorisée		512	
<input checked="" type="checkbox"/>	Longueur maximale d'en-tête générique autorisée		1024	
<input type="checkbox"/>	Longueur maximale Accept autorisée		256	
<input type="checkbox"/>	Longueur maximale Referer autorisée		256	
<input type="checkbox"/>	Longueur maximale Accept-Language autorisée		256	
<input type="checkbox"/>	Longueur maximale Accept-Encoding autorisée		256	
<input type="checkbox"/>	Longueur maximale User-Agent autorisée		256	
<input type="checkbox"/>	Longueur maximale Host autorisée		256	

Débordements de la mémoire tampon

Pour chaque variable de la liste, une entrée numérique indique la taille maximale de la mémoire tampon acceptée par votre serveur Web pour cette variable spécifique. Vous pouvez augmenter ou diminuer cette valeur selon vos besoins propres. Si un client envoie une valeur de variable dont la longueur est supérieure à la limite spécifiée par SecureIIS, la requête sera interdite et journalisée.

Attention : Si vous définissez des valeurs de taille trop faible, vous pourriez désactiver certaines des fonctionnalités de votre site Web. Si cela se produit, augmentez la valeur concernée.

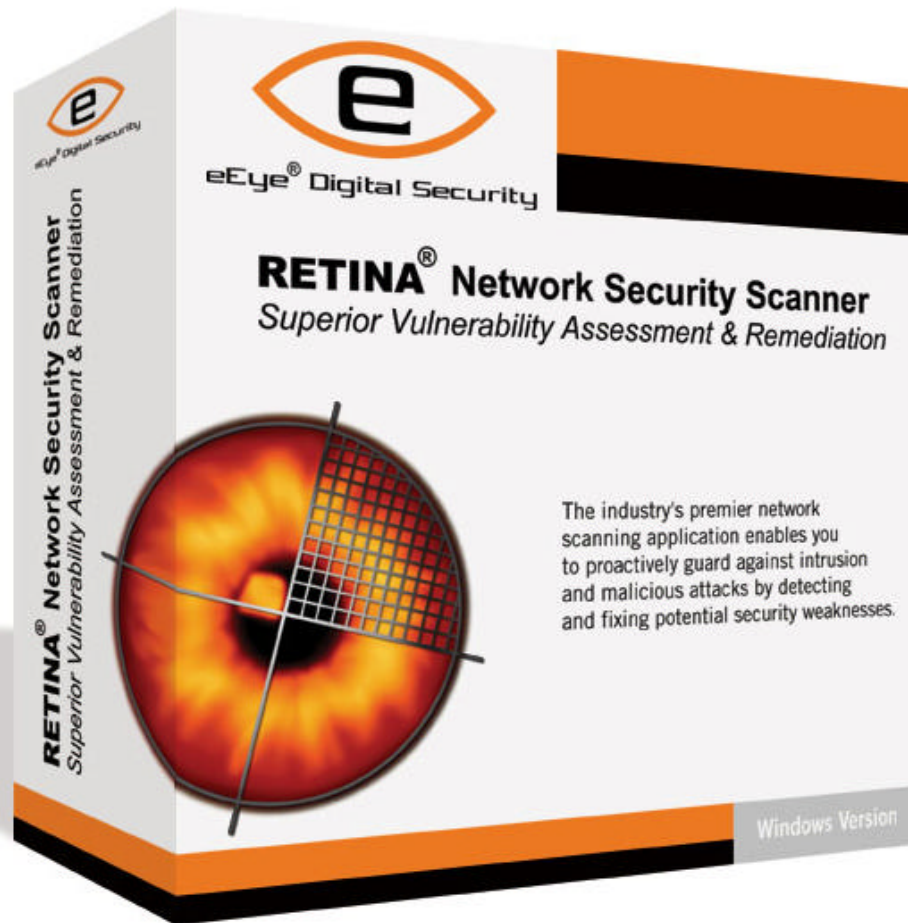
 **Le saviez-vous...**

Le composant Sécurité du site de SecureIIS autorise désormais une configuration spécifique pour chaque dossier.



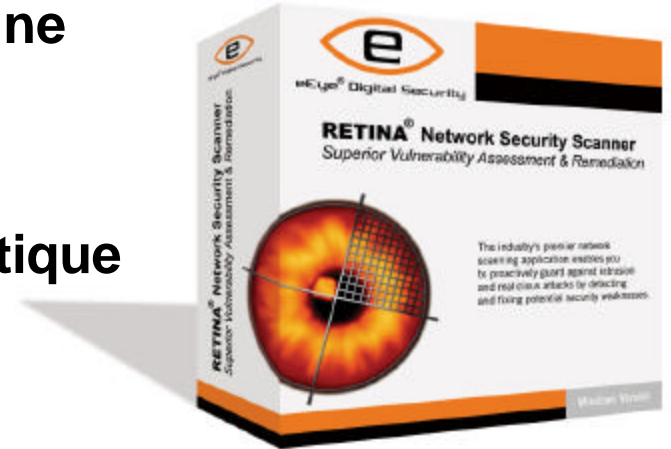
- **Gestion Plus Souple de l'Application des Patchs**
 - Protection Active & Constante des Vulnérabilités connues ou inconnues
- **Protection & Configuration Dynamique**
 - Protection par Politique & Règles (Pas de Signatures)
 - Il n'est Pas Nécessaire de Redémarrer IIS
- **Nouveau Niveau de Sécurité**
 - Pas de Modification de la Configuration de IIS
- **Gestion Centralisée**
 - Politique de Sécurité Globale
 - Centralisation des Logs (REM)





- **Retina : Quelles sont les cibles des audits ?**
 - Serveurs, Stations de travail, firewalls, routeurs, etc.
- **Retina : Audits**
 - Basé sur
 - une adresse IP
 - une plage d'adresses
 - un nom de machine
- **Retina : Résultats**
 - Evaluation du niveau de risque pour chaque vulnérabilité identifiée.
 - Description détaillée des vulnérabilités (descriptif, liens bulletins d'alerte & CVE & Bugtrack)
 - Correctif détaillé pour éradiquer les vulnérabilités (descriptif, liens patches & correction automatique pour certaines vulnérabilités).
 - Rapport détaillé et interactif (HTML) (archivage possible des informations dans un SGBD)

- **#1 Scanner par Network World Magazine**
- **Scanner le plus rapide du marché**
- **Mise à jour automatique**
- **Correctif détaillé & Correction automatique des vulnérabilités**
- **Planificateur**
- **Architecture Ouverte & API pour personnaliser les audits**
- **Rapport personnalisable**
- **CHAM [*Common Hacking Attack Methods*]**
- **Détection complète des OS & Analyse des protocoles**



The screenshot shows the Retina Scanner interface with the following components:

- Machine scannée:** Points to the IP address 192.168.000.077 in the left sidebar.
- Vulnérabilités identifiées:** Points to the list of vulnerabilities in the main pane.
- Niveau de Risque:** Points to the risk level indicator (red diamond) for the selected vulnerability.
- Description de la vulnérabilité sélectionnée:** Points to the detailed description of the 'Registry: LM Hash' vulnerability.
- Correctif détaillé:** Points to the 'Fix it' dialog box.

Category	Description
Registry	Auto Sharing Drive Problem - NT Server
Registry	AutoSharing Drive Problem - NT Wks
Registry	Clear Page File
Registry	MSCHAPv2 VPN
Registry	NTFS 8 Dot 3
Registry	Printer Driver Sec
Registry	Shutdown without Logon
Registry	WinVNC Key Permissions
Remote Access	DCOM Enabled
Remote Access	Dialup Save Password
Remote Access	MS RAS Encrypt
Remote Access	MS RAS Logging
Remote Access	PPP Client Security
Web Servers	Myriad Escaped Characters -W2K
DoS	NT IP Fragment Reassembly -W2K
DoS	Telnet Server Flooding
Mail Servers	MCIS Malformed IMAP Request -W2K
Miscellaneous	NT Reset Browser Frame Vulnerability -W2K
Miscellaneous	NT4 Updated File Fragment Flooding via HTR
Miscellaneous	NT5 Absent Directory Browser Argument
Miscellaneous	NT5 NetBIOS Name Server Protocol Spoofing
Miscellaneous	NT5 Relative Shell Path
Miscellaneous	NT5 Updated File Fragment Flooding via HTR
Miscellaneous	Service Control Manager Named Pipe Impersonation
Miscellaneous	Virtualized UNC Share -W2K
Registry	AEDEBUG Key Perms
Registry	LM Hash

Registry: LM Hash
Description: It is a security risk to send your passwords out over the network using LM (LanMan) authentication. It is recommended that you only use NTLM.
Risk Level: High
How To Fix: Note: Disabling the LM Hash will break functionality with legacy systems, i.e. Windows95/98 machines. To disable the LM hash set the following Registry key settings:
Name: HKLM_LOCAL_MACHINE\Public\System\Control\Control\Kerberos\CompatibilityLevel
Type: REG_DWORD
Value: 2
CVE: CVE-2000-0608

Fix it
Before fixing, make sure you read all details associated with this vulnerability and also make sure you consult your applications vendors to make sure that this fix is compatible with your installed software!
Fix it

Correction automatique proposée

Merci



eEye® Digital Security

Pour plus d'information

Edouard Lorrain : elorrain@eeye.com

Benoît Roussel : broussel@eeye.com

01 58 71 40 31

www.eeye.com

