CERT-UA

Рекомендації
26 листопада 2014

CUA-14-04A
Рекомендації CERT-UA для усунення вразливостей, пов’язаних з використанням протоколу NetBIOS

Державна служба спеціального зв’язку та захисту інформації України
Державний центр захисту інформаційно-телекомунікаційних систем
04119, Україна, м. Київ, вул. Мельникова, 83б
тел.: +380 44 281 88 25
факс: +380 44 489 31 33
www: cert.gov.ua

ЗМІСТ

1. Загальна інформація 3
1.1 Вразливі системи 3
1.2 Інформація про протокол NetBIOS 3
1.3 Типові вразливості протоколу NetBIOS 4
2. Рекомендації 5
2.1 Перевірка на наявність відкритого NetBIOS. 5
2.2 Рекомендації щодо усунення вразливостей протоколу NetBIOS 6
3. Корисні посилання 9

1. Загальна інформація

1.1 Вразливі системи

- Різні версії Windows
- Samba

1.2 Інформація про протокол NetBIOS

NetBIOS (Network Basic Input/Output System) – протокол для роботи в локальних мережах на персональних ЕОМ типу IBM/PC [1]. Був розроблений фірмою Sytek Corporation за замовленням IBM в 1983 році. Він містить у собі інтерфейс сеансового рівня (NetBIOS interface) моделі OSI. Транспортні протоколи — це NetBEUI, TCP/IP, IPX/SPX. NetBIOS over TCP/IP називається NetBT [2].

Мережа Windows не фуцнкціонує без NetBIOS. Неважливо, що у вас написано у властивостях мережевого оточення — якщо є це оточення, значить є і NetBIOS. NetBIOS відповідає за логічні імена комп'ютерів у мережі і передачу даних між двома комп'ютерами, що встановили між собою сесію.

Інтерфейс NetBIOS являє собою стандартний інтерфейс розробки програм (API) для забезпечення мережевих операцій вводу/виводу й керування транспортним протоколом нижчого рівня (transport layer). Програми, що використовують NetBIOS API інтерфейс, можуть працювати тільки при наявності протоколу, що допускає використання такого інтерфейсу**.**

NetBIOS забезпечує:

- Реєстрацію й перевірку мережевих імен
- Встановлення й розрив з'єднань
- Зв'язок із гарантованою доставкою інформації
- Зв'язок з негарантованою доставкою інформації
- Підтримку керування й моніторингу драйвера й мережевої карти

NetBIOS використовує порти:

- 137/tcp, 137/udp – для служби імен (Name Service)
- 138/tcp, 138/udp – для служби дейтаграм (Datagram Service)
- 139/tcp, 139/udp – для сесій (Session Service)

Детальна реалізація протоколу описана в

- RFC 1001
- RFC 1002

1.3 Типові вразливості протоколу NetBIOS.

Доступ із віддаленого комп'ютера, запис/зчитування з нього

За допомогою вразливостей NetBIOS зловмисник може отримати доступ до віддаленого комп'ютера, це відкриває йому доступ до файлів жертви, також зловмисник може завантажувати файли (наприклад шкідливі файли, які містять віруси) на комп'ютер жертви, або виконувати на ньому довільні команди.

Відмова в обслуговувані(DoS).

Зловмисник може за допомогою спеціальних підроблених запитів, які відправляються на комп'ютер жертви, заборонити йому приймати будь-який NetBIOS трафік, що приведе до відмови в обслуговувані. Так, наприклад, у Windows Server 2008 та Windows 7 можливо за допомогою протоколу SMB викликати відмову в обслуговувані (нескінченний цикл, зависання системи) через SMBv1 або SMBv2 відповідь, яка містить неправильне значення довжини в заголовку NetBIOS.

Нижче приведено список вразливостей. Опис цих вразливостей ви можете знайти на сайті https://cve.mitre.org/:

- CVE-2014-3560
- CVE-2009-3676
- CVE-2009-0094
- CVE-2007-5398
- CVE-2005-1216
- CVE-2003-0661

2. Рекомендації

2.1 Перевірка на наявність відкритого NetBIOS.

Для перевірки того чи працює на комп'ютері NetBIOS, відкрийте командну строку і введіть команду:

nbtstat –a "IP-адреса комп'ютера"

Якщо NetBIOS запущений ви побачите приблизно таку відповідь:

NetBIOS Remote Machine Name Table

Name		Type	Status
USER-PC	<00>	UNIQUE	Registered
WORKGROUP	<00>	GROUP	Registered
USER-PC	<20>	UNIQUE	Registered
WORKGROUP	<1E>	GROUP	Registered

Якщо NetBIOS вимкнутий, або порт 139 заблокований, ви отримаєте відповідь "Host not found".

2.2 Рекомендації щодо усунення вразливостей протоколу NetBIOS

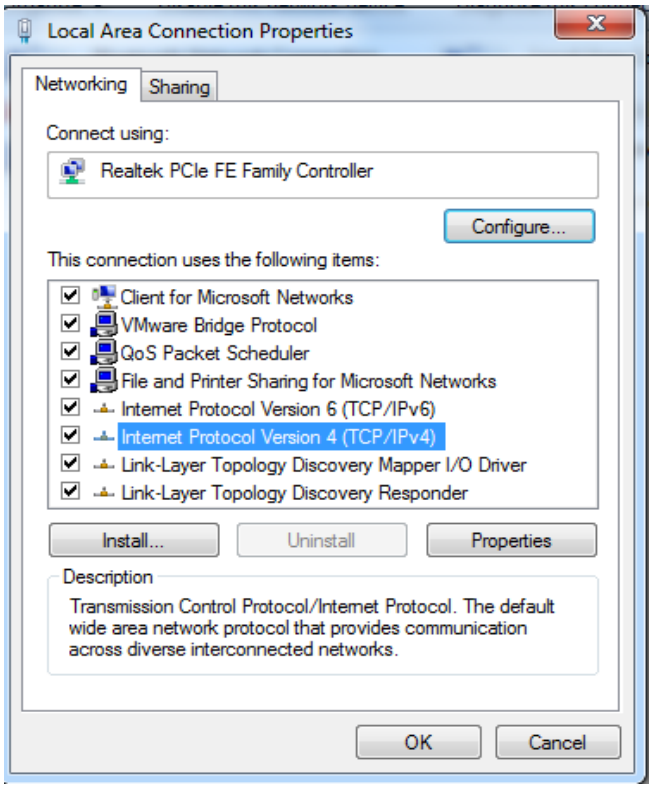
Вхідна фільтрація

Обмежте доступ до сервісу NetBIOS користувачам із зовнішньої мережі за допомогою брандмауеру. Для цього забороніть доступ із зовнішньої мережі до портів 137/tcp, 137/udp, 138/tcp, 138/udp, 139/tcp, 139/udp. Зверніть увагу на те, що такі дії запобігають отриманню NetBIOS трафіку з мережі Інтернет, але не заважають локальним користувачам використовувати ці вразливості. Рекомендується, навіть якщо ви не використовуєте послуги NetBIOS, заблокувати ці порти, якщо в них немає явної потреби.

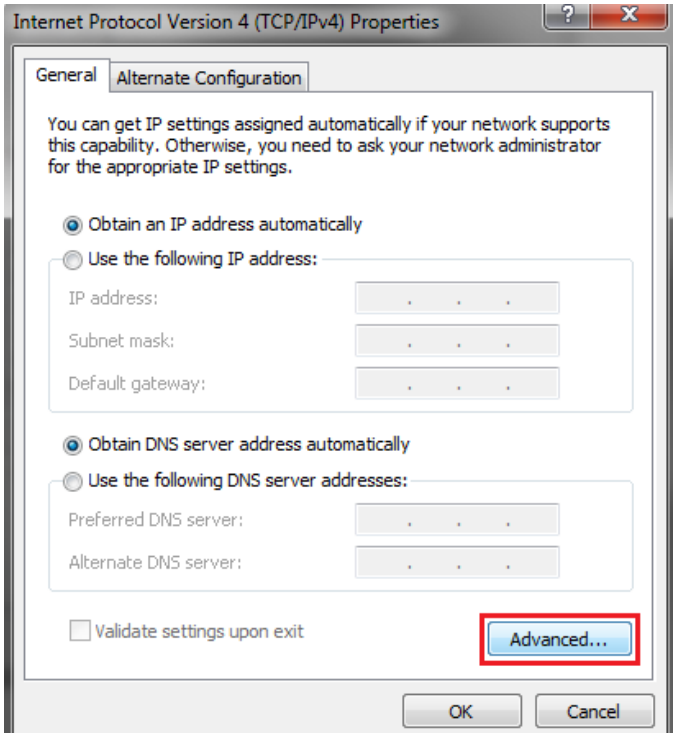
Відключення сервісу NetBIOS

Попередження: Впевніться що відключення сервісу не вплине на вашу роботу.

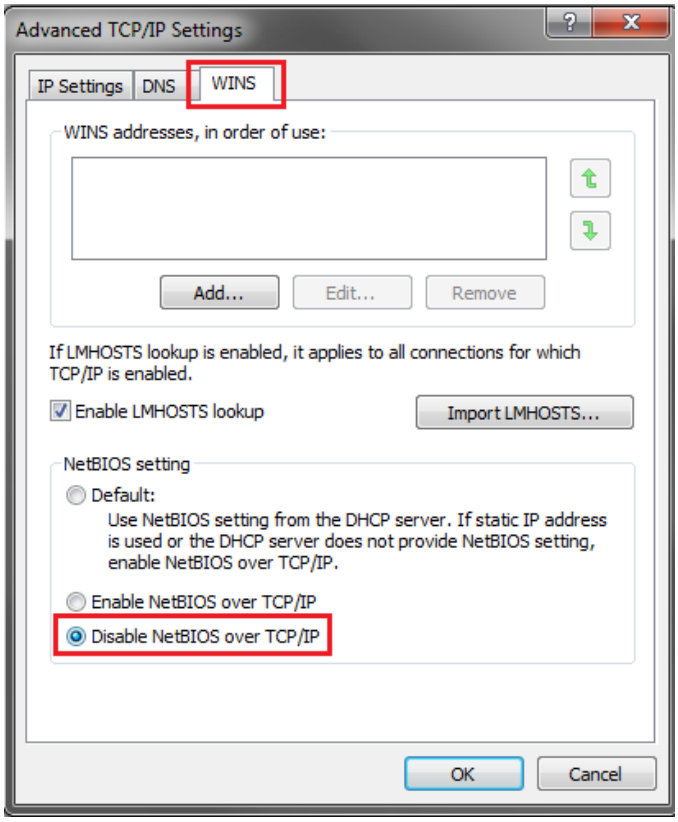
1. Відкрийте "Control Panel" в меню Пуск
2. Оберіть "Network And Sharing Center"
3. Оберіть "Change Adapter Settings"
4. Правий клік мишки на ваш мережевий адаптер та оберіть "Properties" (Властивості)
5. У відкритому вікні оберіть "Internet Protocol Version 4" і "Properties"



6. Після цього обираєте опцію "Advanced"



7. Переходьте до вкладки "WINS" та обираєте "Disable NetBIOS over TCP/IP"



Використовуйте стійкі паролі

Обов’язково використовуйте пароль для входу в систему. Використовуйте стійкий пароль. Це ускладнить отримання зловмисником віддаленого доступу до вашої системи. Більш детально про це написано тут [9].

Використовуйте оновлення

Відвідайте сайт Microsoft для інформації щодо оновлень для вашої версії ОС, які виправляють вразливості пов’язані з використанням NetBIOS. Також, рекомендується використовувати сучасні версії ОС сімейства Windows, для яких здійснюється підтримка і виходять періодичні оновлення (наприклад, Windows 7 і вище).

Якщо ви користуєтесь програмою Samba, то оновіть її до актуальної версії. Так, наприклад, вразливість CVE-2014-3560 була виправлена у версії 4.1.11.

3. Корисні посилання

[1] https://en.wikipedia.org/wiki/NetBIOS

[2] https://en.wikipedia.org/wiki/NetBIOS_over_TCP/IP

[3] http://www.kb.cert.org/vuls/id/32650

[4] https://technet.microsoft.com/ru-ru/library/security/dn631936.aspx

[5] https://cve.mitre.org

[6] http://www.opennet.ru/docs/RUS/inet_book/4/42/nbio_423.html

[7] http://www.ietf.org/rfc/rfc1001.txt

[8] http://www.ietf.org/rfc/rfc1002.txt

[9] http://cert.gov.ua/?p=1536

Зміни до документу

- 26.11.2014 – перший випуск.