CUA-14-03A
Рекомендації CERT-UA для усунення вразливостей, пов’язаних з використанням протоколу SSDP

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

1.1 Загальна інформація

SSDP (англ. Simple Service Discovery Protocol – Простий протокол виявлення сервісів) – мережевий протокол, який описує механізм виявлення різноманітних мережевих сервісів та пристроїв [1]. SSDP є основою протоколу виявлення пристроїв в мережі UPnP. Домашні маршрутизатори, як правило, виявляються комп’ютерами за допомогою SSDP. Для відображення інформації про маршрутизатори та медіа-сервери в мережі, ці прилади також повинні підтримувати протокол HTTP, оскільки SSDP повідомляє комп’ютеру http-посилання на вузол керування приладом.

SSDP в якості транспортного протоколу використовує UDP як в одноадресній, так і в багатоадресній розсилці для виявлення пристроїв в мережі, посилаючи запити на спеціальну мультикаст IP-адресу 239.255.255.250 на UDP-порт 1900. Кожний прилад мережі, який підтримує SSDP, повинен відповісти на запит, повідомивши у відповіді http-посилання на сторінку управління приладом.

SSDP використовується великою кількістю мережевих приладів, таких як маршрутизатори, принтери, веб-камери, smart-TV, принтери і т. д.

UPnP (англ. Universal Plug and Play) – набір мережевих протоколів, які призначені для підтримки автоматичного пошуку та налаштування пристроїв в домашніх та невеликих корпоративних мережах [2]. Більшість різноманітних розробників випускають прилади з підтримкою UPnP. В цих приладах UPnP ввімкнутий за замовчанням.

1.2 Типові вразливості протоколу SSDP

В приладах, які підтримують роботу протоколу SSDP було знайдено декілька типів вразливостей. Це вразливості до атак з використанням переповнення буферу та до участі у атаках типу SSDP-amplification. Оскільки більшість приладів взаємодіє з UPnP через WAN (глобальну комп'ютерну мережу), це робить їх вразливими до атак з мережі Інтернет.

Вразливість до участі у DDoS-атаках SSDP-amplification

Для обміну інформацією між UPnP пристроями використовується протокол SOAP (простий протокол доступу до об'єктів). На першому етапі атаки зловмиснику потрібно зібрати інформацію про прилади, які працюють з включеним UPnP [3]. Для цього зловмисник відправляє SOAP-запит M-SEARCH на UDP-порт 1900 певної кількості IP-адрес. Зазвичай, коли в мережу підключається новий прилад підтримуючий UPnP, для того щоб дізнатись, які сервіси UPnP підтримуються в мережі, він відсилає запит M-SEARCH на мультикаст адресу 239.255.255.250 на UDP-порті 1900. Це повідомлення містить заголовок схожий на HTTP-запит [11].

```
M-SEARCH * HTTP/1.1
HOST: 239.255.255.250:1900
MAN: ssdp:discover
MX: 10
ST: ssdp:all
```

Всі інші прилади, або програми мережі, які використовують UPnP, посилають відповідь на цей запит, яка містить інформацію про місцезнаходження XML-файлу описання приладу. За допомогою цієї відповіді новий прилад дізнається, які UPnP прилади та програми працюють в мережі.

```
HTTP/1.1 200 OK
CACHE-CONTROL:max-age=1800
EXT:
LOCATION:http://10.0.0.138:80/IGD.xml
SERVER:SpeedTouch 510 4.0.0.9.0 UPnP/1.0 (DG233B00011961)
ST:urn:schemas-upnp-org:service:WANPPPConnection:1
USN:uuid:UPnP-SpeedTouch510::urn:schemas-upnp-org:service:WANPPPConnection:1
```

Важливо знати те, що відповіді від приладів відправляються за допомогою UDP на IP-адресу з якої прийшов запит, тобто якщо зловмисник відправить такий запит, то вся інформація про прилад прийде до нього.

Зібравши певний перелік вразливих приладів, зловмисник відправляє SOAP-запити із заміною дійсної IP-адреси джерела запиту IP-адресою жертви до UPnP пристрою. Оскільки робота SSDP базується на використані UDP-протокола, який не вимагає встановлення з'єднання, і працює без збереження стану про з'єднання (stateless), то підміна IP-адреси є можливою. Коли пристрій відправляє відповідь, вона приходить на IP-адресу жертви. Коефіцієнт підсилення залежить від змісту XML-файлу опису приладу. Використовуючи бот-мережу зловмисник може згенерувати велику кількість підроблених запитів і ,таким чином, з легкістю створити велику кількість трафіку направленого на адресу жертви [4].

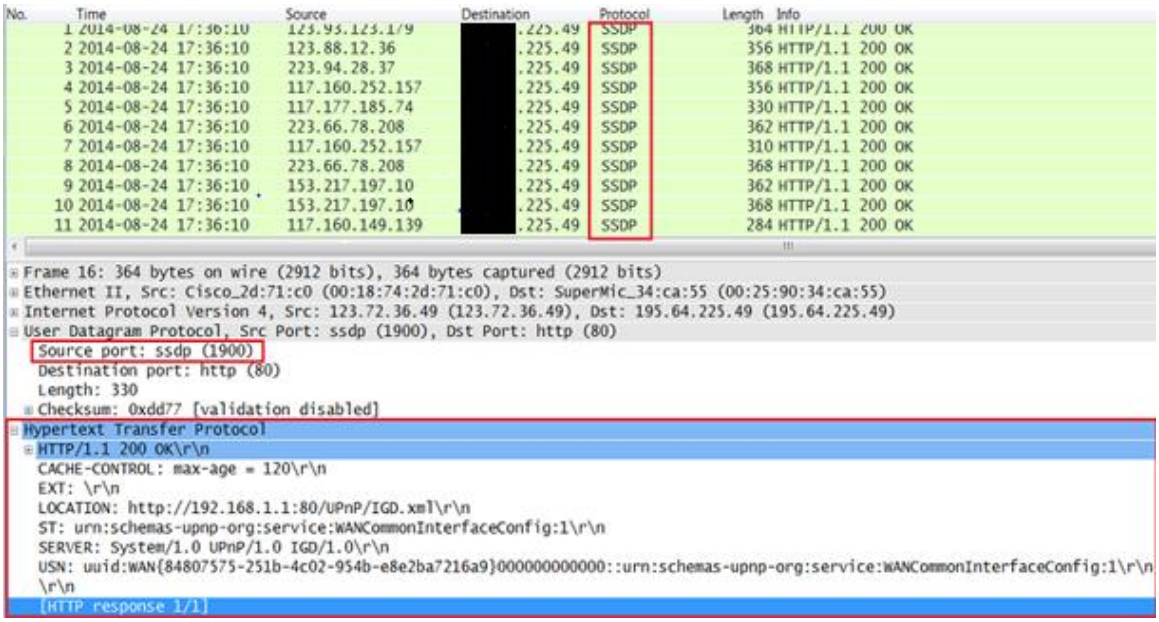

Рис 1. Приклад атаки SSDP-amplification

Вразливість до атак переповнення буферу в стеку

CERT/CC та Rapid7 повідомляють, що SDK для UPnP-приладів містить багаточисленні вразливості до атак переповнення буферу в реалізації бібліотеки libupnp [5], [6]. Пристрої, які використовують libupnp можуть приймати UPnP-запити з Інтернету, що робить вразливості доступними всім користувачам Інтернету.

Бібліотека libupnp вразлива до переповнення буферу стеку при прийомі шкідливих SSDP-запитів. Вразливими версіями є 1.2 (Intel SDK) та 1.2.1a – 1.8.0(Portable SDK), в яких за допомогою функції unique_service_name(), яка призначена для обробки вхідних SSDP-запитів на UDP-порт 1900, можливо здійснити атаку переповнення буферу. Нижче приведено список вразливостей. Опис цих вразливостей ви можете знайти на сайті https://cve.mitre.org/:

1. CVE-2012-5958
2. CVE-2012-5959
3. CVE-2012-5960
4. CVE-2012-5961
5. CVE-2012-5962
6. CVE-2012-5963
7. CVE-2012-5964
8. CVE-2012-5965
9. CVE-2013-0229
10. CVE-2013-0230

На даний момент найновіша версія libupnp – 1.6.17, в якій виправлено ще не всі вразливості.

Інформація про виробників

Велика кількість компаній використовують цю бібліотеку в своїй продукції, багато з якої є домашні маршрутизатори. Майже всі пристрої, які використовують libupnp, є вразливими до атак переповнення буферу. CERT/CC проінформував більше 200 виробників які використовують libupnp в своїй продукції. Нижче приведено список таких виробників [7].

Vendor	Status	Date Notified	Date Updated
Axis	Affected	13 Dec 2012	05 Apr 2013
Cisco Systems, Inc.	Affected	13 Dec 2012	29 Jan 2013
D-Link Systems, Inc.	Affected	13 Dec 2012	31 Jan 2013
Fujitsu Technology	Affected	10 Jan 2013	29 Jan 2013
Huawei Technologies	Affected	13 Dec 2012	29 Jan 2013
Ipitomy	Affected	08 Jan 2013	01 Feb 2013
Linksys	Affected	13 Dec 2012	29 Jan 2013
NEC Corporation	Affected	13 Dec 2012	29 Jan 2013
Siemens	Affected	13 Dec 2012	30 Jan 2013
Sony Corporation	Affected	13 Dec 2012	30 Jan 2013
Synology	Affected	3 Dec 20122	8 Feb 2013

• Teldat	Not Affected		05 Feb 2013
• Ubiquiti Networks	Not Affected	09 Jan 2013	29 Jan 2013
• Yamaha Corporation	Not Affected	-	01 Feb 2013
• 3com Inc	Unknown	13 Dec 2012	29 Jan 2013
• Belkin, Inc.	Unknown	13 Dec 2012	29 Jan 2013
• Debian GNU/Linux	Unknown	13 Dec 2012	29 Jan 2013
• EMC Corporation	Unknown	13 Dec 2012	9 Jan 2013
• Geexbox	Unknown	11 Jan 2013	29 Jan 2013
• Intel Corporation	Unknown	01 Feb 2013	01 Feb 2013
• Koukaam	Unknown	10 Jan 2013	29 Jan 2013
• Logitech	Unknown	04 Jan 2013	29 Jan 2013
• Motorola, Inc.	Unknown	13 Dec 2012	29 Jan 2013
• Netgear, Inc.	Unknown	13 Dec 2012	29 Jan 2013
• orb Networks	Unknown	16 Jan 2013	29 Jan 2013
• Pantech North America	Unknown	13 Dec 2012	29 Jan 2013
• Red Hat, Inc.	Unknown	04 Dec 2012	29 Jan 2013
• SFR	Unknown	04 Jan 2013	29 Jan 2013
• Sitecom	Unknown	04 Jan 2013	29 Jan 2013
• SMC Networks, Inc.	Unknown	04 Jan 2013	29 Jan 2013
• Texas Instruments	Unknown	13 Dec 2012	29 Jan 2013
• TP-Link	Unknown	04 Jan 2013	29 Jan 2013
• Ubuntu	Unknown	04 Dec 2012	29 Jan 2013
• Visual Tools	Unknown	10 Jan 2013	29 Jan 2013
• ZyXEL	Unknown	13 Dec 2012	29 Jan 2013

2. Рекомендації

2.1 Перевірка на наявність відкритого SSDP.

Є декілька організацій, які пропонують безкоштовні веб-інструменти сканування для перевірки наявності вразливостей пов'язаних з використанням SSDP:

http://www.openssdpproject.org/

http://upnp-check.rapid7.com/

2.2 Рекомендації щодо усунення вразливостей протоколу SSDP

Вхідна фільтрація

Потрібно заборонити доступ до UPnP-приладів користувачам із мережі Інтернет. Для цього необхідно налаштувати брандмауер на фільтрацію вхідного трафіку, який надходить на UDP-порт 1900. Окрім цього мережевого порту (як src.port) є доцільним відфільтровувати 123 і 53 порти, адже вони також використовуються у DDoS-атаках, що здійснюються з використанням техніки підсилення (amplification). Для того, щоб ефективно впровадити цей механізм, правила фільтрації слід застосовувати, в першу чергу, провайдерам, які знаходяться вище за «мережевою ієрархією».

Вимкнення UPnP

Рекомендується виключити підтримку UPnP на мережевих пристроях, якщо в ньому немає безпосередньої потреби.

Використовуйте оновлення

Зв'яжіться з поставником ваших UPnP-пристроїв, або відвідайте їх веб-сайт для пошуку інформації про наявність оновлення, які виправляють вищевказані вразливості.

3. Корисні посилання

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

[2] https://en.wikipedia.org/wiki/Universal_Plug_and_Play

[3]http://www.prolexic.com/kcresources/prolexic-threat-advisories/ssdp-reflection-attacks-cybersecurity-locked/ssdp-reflection-attacks-cybersecurity-US-101514-locked.pdf

[4] http://cert.gov.ua/?p=1577

[5] http://www.kb.cert.org/vuls/id/922681

[6] https://community.rapid7.com/docs/DOC-2150

[7]http://www.kb.cert.org/vuls/byvendor?searchview&Query=FIELD+Reference=922681&SearchOrder=4

[8] http://upnp-check.rapid7.com/

[9] http://www.openssdpproject.org/

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

[11] http://www.upnp-hacks.org/upnp.html

[12] http://www.kb.cert.org/vuls/id/357851

Зміни до документу

- 26.11.2014 – перший випуск.