Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S . G . D . S . N
Agence nationale de la sécurité des systèmes d'information
CERT-FR

Paris, le 22 août 2016
N° CERTFR-2016-ACT-034

Affaire suivie par :
CERT-FR

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTFR-2016-ACT-034

1 - Ra-Guard

Dans la majorité des réseaux actuels, IPv4 est utilisé et les hôtes effectuent des requêtes DHCP pour obtenir les paramètres de configuration réseau (adresse, passerelle, serveur DNS, etc.). Une des fonctionnalités apportées par IPv6 est la possibilité d'autoconfigurer les hôtes, en utilisant le mécanisme SLAAC (Stateless Address Autoconfiguration). Lorsque ce mécanisme est utilisé, c'est le routeur qui annonce les paramètres de configuration réseau aux hôtes au travers de messages ICMPv6 RA (Router Advertisement). De même que les hôtes effectuent généralement des requêtes DHCP par défaut en IPv4, ils sont généralement à l'écoute de messages RA par défaut en IPv6. Ce mécanisme présente l'avantage de pouvoir fournir une connectivité IPv6 aux hôtes, sans utiliser de serveur DHCP, mais uniquement un routeur. Cependant, il peut aussi présenter des risques, parmi lesquels nous pouvons citer :

1. dans un réseau IPv6, une personne malveillante peut émettre des messages RA spécialement conçus (avec une préférence supérieure à celle des messages RA légitimes notamment) dans le but de se faire passer pour le routeur par défaut et intercepter des flux réseau ;
2. dans un réseau IPv4-only, une personne malveillante peut émettre des messages RA dans le but de fournir une connectivité IPv6 aux hôtes et intercepter des flux réseau [1] ;
3. lorsque le partage de connexion Internet de Windows, ICS (Internet Connection Sharing), d'un hôte est activé, des messages RA sont émis et la connectivité des autres hôtes peut être perturbée.

Pour se prémunir contre ces désagréments, le mécanisme RA-Guard, normalisé dans le RFC 6105 [2], peut être utilisé. RA-Guard est à implémenter au niveau des commutateurs en définissant quels sont les ports sur lesquels sont branchés les routeurs autorisés à émettre des messages RA. Éventuellement, les paramètres des messages RA autorisés peuvent être définis.

Voici un exemple de configuration sur un commutateur Cisco pour lequel un routeur légitime est branché sur le port GigabitEthernet 1/0/1 et des hôtes sont branchés sur les ports GigabitEthernet 1/0/2 à GigabitEthernet 1/0/50 :

```
routeur>enable
Password:
routeur#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
routeur(config)#interface range GigabitEthernet 1/0/2-50
routeur(config-if-range)#ipv6 nd raguard
```

Les commandes ci-dessous peuvent être utilisées pour vérifier que RA-Guard est bien actif et si des messages RA sont bloqués :

```
routeur#show ipv6 nd raguard policy default
Policy default configuration:
device-role host
Policy default is applied on the following targets:
```

```
Target Type Policy Feature Target range
Gi1/0/2 PORT default RA guard vlan all
Gi1/0/3 PORT default RA guard vlan all
Gi1/0/4 PORT default RA guard vlan all
[...]
```

```
routeur#show ipv6 snooping counters interface GigabitEthernet 1/0/5
Received messages on Gi1/0/5:
Protocol Protocol message
NDP RA33
DHCPv6

Bridged messages from Gi1/0/5:
Protocol Protocol message
NDP
DHCPv6

Dropped messages on Gi1/0/5:
Feature Protocol Msg [Total dropped]
RA guard NDP RA [33]
reason: Message unauthorized on port [33]
```

Cette configuration réduit donc les risques de perturbation des hôtes dus à des messages RA non désirés. Même dans un réseau IPv4, RA-Guard présente un intérêt pour faire face aux cas 2 et 3 ci-dessus. Dans un tel réseau, RA-Guard pourra être activé sur tous les ports.

RA-Guard étant un mécanisme assez récent, il n'est pas supporté par tous les commutateurs. L'outil Cisco Feature Navigator [3] de Cisco et Feature Explorer [4] de Juniper permettent de connaître les commutateurs de ces marques supportant ce mécanisme. Le RFC 6104 [5] et la Newsletter HSC n99 [6] proposent des solutions permettant de se protéger contre les RA non désirés sans utiliser RA-Guard.

Documentation

1 Bulletin d'actualité CERTFR-2014-ACT-013
http://cert.ssi.gouv.fr/site/CERTFR-2014-ACT-013/

2 RFC 6105 - IPv6 Router Advertisement Guard
https://tools.ietf.org/html/rfc6105

3 Cisco Feature Navigator - Cisco Systems
http://www.cisco.com/go/cfn

4 Feature Explorer - Juniper Networks
https://pathfinder.juniper.net/feature-explorer/

5 RFC 6104 - Rogue IPv6 Router Advertisement Problem Statement
https://tools.ietf.org/html/rfc6104

6 [Newsletter HSC] N99 - Novembre 2012
http://www.hsc-news.com/archives/2012/000100.html

2 - Rappel des avis émis

Dans la période du 15 au 21 août 2016, le CERT-FR a émis les publications suivantes :

- CERTFR-2016-ALE-005 : Multiples vulnérabilités dans les pare-feux Cisco
- CERTFR-2016-AVI-282 : Multiples vulnérabilités dans les produits VMware
- CERTFR-2016-AVI-283 : Vulnérabilité dans le micrologiciel Fortigate de Fortinet
- CERTFR-2016-AVI-284 : Multiples vulnérabilités dans les produits Cisco

Gestion détaillée du document

22 août 2016 version initiale.

Conditions d'utilisation de ce document :	`http://cert.ssi.gouv.fr/cert-fr/apropos.html`
Dernière version de ce document :	`http://cert.ssi.gouv.fr/site/CERTFR-2016-ACT-034`