INTERNET-DRAFT
Intended Status: Informational
Expires: April 12, 2015

M.Nakatani
JPCERT/CC
Y.Kitaguchi
Kanazawa University
K.Nagami
M.Kosugi
R.Hiromi
INTEC Inc.
October 9, 2014

Introducing IPv6 vulnerability test program in Japan
draft-jpcert-ipv6vullnerability-check-01

Abstract

Japan Computer Emergency Response Team Coordination Center, known as JPCERT/CC have been researching about vulnerability in use of IPv6 and provided the information toward vendors in Japan. They also verified to occur the security incident with several products.

In 2013, JPCERT/CC called for vendors to participate their IPv6 security program. JPCERT/CC collects the results of equipments and open to the public for an user reference of procurement.

In this document we describe about the program to share the experimental activity.

Status of this Memo

Copyright and License Notice

Table of Contents

1 Introduction 3
1.1 Requirements Language 3
2 Terminology 3
3 IPv6 Vulnerability Test Program 4
3.1 Test Concept and requirement 4
3.2 Test Items and its Criteria 4
3.3 Providing Test Tools and Manual 6
3.4 Handling results 6
4 Conclusion 7
5 Security Considerations 8
6 IANA Considerations 8
7 Acknowledgements 8
8 References 9
8.1 Normative References 9
8.2 Informative References 9
Appendix A: IPv6 vulnerability reference RFCs and i-Ds 10
Authors' Addresses 15

1 Introduction

JPCERT/CC started "The IPv6 Security Test" in Japan in 2013. The target equipments are routers and to verify their ability for the protection of vulnerabilities which are pointed out in RFC or Internet-Drafts. JPCERT/CC focuses exclusively on the possible attacks coming from the Internet. Providing test materials(tool and document), JPCERT/CC collects the results from vendors and published IPv6 Security Test respondent product List. This list is keeping to be up to date. In this document we describe about the program to share the experimental activity.

1.1 Requirements Language

Take careful note: Unlike other IETF documents, the key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are not used as described in RFC 2119 [RFC2119]. This document uses these keywords not strictly for the purpose of interoperability, but rather for the purpose of establishing industry-common baseline functionality. As such, the document points to several other specifications (preferable in RFC or stable form) to provide additional guidance to implementers regarding any protocol implementation required to produce a successful CE router that interoperates successfully with a particular subset of currently deploying and planned common IPv6 access networks.

2 Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

3 IPv6 Vulnerability Test Program

3.1 Test Concept and requirement

This test program is focused on exclusively on the inbound attacks which possibly caused at WAN port(then through LAN port). JPCERT/CC narrowed down 15 items out of 80[Appendix.A]. Fig.1 shows basic network topology. In this test. Basically test packets sent to both LAN and WAN then confirm the robustness.

Figure.1 Basic Network Topology

```
                      +---------------+
                      | IPv6 Attacker |
                      +---------------+
                                |
                                |
         +--------------- IPv6 Internet ----------------------+
                                |
                                |
                        +----@--------+
                        | User Router |
                        +----@--------+
                                |
                                |
         +----------------  /64 prefix segment ---------------+
                      |         |        |        |
                      |         |        |        |
                   +------+ +------+ +------+ +------+
                   |Client| |Client| |Client| |Client|
                   +------+ +------+ +------+ +------+
```

3.2 Test Items and its Criteria

Here is 15 test items.

[01] Disabling type 0 routing header processing
[02] Protection for a DoS attack on the router by hop-by-hop option header
[03] Protection for unexpected jumbo packet by extra large payload option
[04] Corresponding completely overwrite packet information by unauthorized fragment header(overlap-first-zero fragmentation)
[05] Corresponding completely overwrite packet information by unauthorized fragment header(overlap-last-zero fragmentation)
[06] Corresponding partially overwrite packet information by

unauthorized fragment header(overlap-first-hop fragmentation)
[07] Corresponding partially overwrite packet information by
unauthorized fragment header(overlap-last-hop fragmentation)
[08] Detection of a DoS attack by tiny fragment header
[09] Protection for tiny fragment of a DoS attack with a large
amount of using the small fragment header
[10] Protection for a DoS attack by transmitting the first
fragmented packet only
[11] Protection for a DoS attack by single fragmented packet
using atomic fragment
[12] Protection for a DoS attack by single fragmented packet
with a large amount of atomic fragments
[13] Protection for an attack from the off-path attacker by fragment
ID prediction
[14] Protection for a DoS attack to the router using the neighbor
discovery service
[15] Protection for a DoS attack by sending a large number of
broken packets to the router

Table.1 Type of Attack and Criteria for the evaluation

No.	Type of Attack	Criteria
01	DoS Attack packet filtering evasion	comply the DoS resistance policy(*) discard packet or error reply
02	DoS Attack	comply the DoS resistance policy(*)
03	DoS Attack	comply the DoS resistance policy(*)
04	packet filtering evasion	discard packet or error reply
05	packet filtering evasion	discard packet or error reply
06	packet filtering evasion	discard packet or error reply
07	packet filtering evasion	discard packet or error reply
08	DoS Attack	comply the DoS resistance policy(*)
09	DoS Attack	comply the DoS resistance policy(*)
10	DoS Attack	comply the DoS resistance policy(*)
11	DoS Attack	comply the DoS resistance policy(*)

12	DoS Attack	comply the DoS resistance policy(*)
13	DoS Attack	comply the DoS resistance policy(*)
14	DoS Attack	comply the DoS resistance policy(*)
15	DoS Attack	comply the DoS resistance policy(*)

(*) the DoS resistance policy

Router that "PASSED" this test has ability with all the result in the below.

1. do not reboot
2. do not hung-up
   (slow-down will be acceptable)
3. return to the original condition after DoS attack stopped
   (to see the condition of the router, ping to the router
   from a connected node)

3.3 Providing Test Tools and Manual

JPCERT/CC provides a testing tool to an applicant developer due to execute these test at same procedure and methodology. Prior to the open up this test program JPCERT/CC examined test cases itself and test tool with open source software then combined some software into a distribution tool.

Current test tool includes these software ; - THC IPv6 Toolkit 2.3THC IPv6 Toolkit 2.3 - SI6 Networks IPv6 ToolKit v1.4.1 - nmap 6.40 - WireShark Version 1.2.15 - minicom

slight modification was made to the software to fix for the test cases.

JPCERT/CC also provides a technical guide and an manual. The technical guide is can be downloaded from their Web page[WEB] for the general test guide to public.

3.4 Handling results

JPCERT/CC asks for the result of the test from associate participants. Results are listed and released in the JPCERT/CC's web site[WEB] under an agreement. JPCERT/CC updates the list continually when they gets new information.

4 Conclusion

IPv6 is in the way of universal deployment. In Japan, an organization named JPCERT/CC started to provide a IPv6 related security evaluation program. After one year of the activity, JPCERT/CC also publish the result of test. End users of small and mid-sized companies or SIers can refer the list for an procurement even if they have lack of knowledge about IPv6 and its security consideration. For the vendors, they can develop IPv6 secure appraisal product that suited for targeted companies in base line.

The benefit of this activity is;

(1) developer and JPCERT/CC
JPCERT/CC is able to informed possible threats to vendors proactively. Vendors are able to create more safer products in advance. This scheme changes incident-first to information-first approach.

(2) customer
Especially for a small and mid-sized companies, they are going to start to adopt IPv6 easier if they don't have much knowledge.

Currently JPCERT/CC defined 15 items for the test case. Beyond controversy they will review and enhance the test program from time to time.

5 Security Considerations

Possible security threats are same as what pointed out in original protocols and technologies referred in this document.

6 IANA Considerations

This document has no actions for IANA.

7 Acknowledgements

Thanks for the following vendors/organizations with the contribution of this activity.

IPv6 Promotion Council, Brocade Communications Systems Inc., NEC Platforms, Ltd., Furukawa Electric Co., Ltd.,Hitachi Metals, Ltd, CENTURY SYSTEMS Co.,Ltd and Codenomicon.

8 References

8.1 Normative References

TBD

8.2 Informative References

[WEB] JPCERT/CC, IPv6 Security Test Appraisal List, September 2014, <https://www.jpcert.or.jp/research/ipv6product_list.html>.

Appendix A: IPv6 vulnerability reference RFCs and i-Ds

Here is possible threats list and related RFC and internet-drafts.

1. Basic Header/Extension Header definition

1-1 Access filtering policy evasion using by Type 0 Routing Header,
RFC4942;RFC5095;RFC5871
1-2 DoS attack caused by Type 0 Routing Header,
RFC4942;RFC5095;RFC5871
1-3 DoS attack caused by Hop by Hop Option Header,
RFC4942
1-4 Handling problem and resource management problem of jumbogram,
RFC4942
1-5 Packet overwrite by unauthorized fragment header,
RFC4942;RFC5722
1-6 DoS attack caused by tiny fragmented packets,
RFC7112
1-7 Abuse by receiving a lot of first fragment packets
1-8 DoS attack caused by atomic fragment header,
RFC6946
1-9 DoS attack caused by prediction of fragment identification values,
draft-ietf-6man-predictable-fragment-id-01
1-10 Distinctiveness on firewall implementation for packet reassembly,
RFC4942;RFC7112;RFC5722
1-11 Implementation problems in processing extension header chain;
RFC4942;RFC7112;RFC5722
1-12 Implementation problems in Unknown Headers/Destination Options,
RFC4942;RFC6564
1-13 Abuse using by Pad1 and PadN Options in Hop-by-Hop and Destination option headers,
RFC4942
1-14 DoS attack using by old specification of Flow Label,
RFC3697;RFC6437
1-15 Covert Channel using by Flow Label,
RFC6437;draft-gont-6man-flowlabel-security-03
1-16 Information Leaking by Flow Label,
RFC6437;draft-gont-6man-flowlabel-security-03

2. NDP (link layer address resolution)

2-1 Neighbor Solicitation/Advertisement Spoofing,
RFC3756;RFC6980
2-2 Neighbor Unreachability Detection (NUD) failure,
RFC3756;RFC6980

2-3 Duplicate Address Detection DoS Attack,
RFC3756;RFC6980;draft-ietf-6man-enhanced-dad-06
2-4 Neighbor Discovery DoS Attack,
RFC3756;RFC4942
2-5 Abuse on Neighbor cache table,
RFC3756;RFC4942

3. NDP (address auto-configuration)

3-1 Juggled default route,
RFC3756;RFC6104;RFC6105;RFC7113
3-2 Juggled prefixes,
RFC3756;RFC6104;RFC6105;RFC7113
3-3 Juggled DNS server information,
RFC3756;RFC6104;RFC6105;RFC6106;draft-gont-6man-slaac-dns-config-issues-00
3-4 Sniffing caused by following old specification of on-link assumption,
RFC3756;RFC4943;RFC6104;RFC6105;RFC6583;RFC7113
3-5 Parameter Spoofing,
RFC3756;RFC6104;RFC6105;RFC7113
3-6 DoS attack caused by Router Advertisement,
RFC3756;RFC6104;RFC6105;RFC7113
3-7 Filtering Policy Evasion by fragment packets
RFC7113;RFC5722

4. ICMPv6

4-1 Spoofed Redirect Message,
RFC3756;draft-gont-opsec-ipv6-nd-shield-00;RFC6980
4-2 DoS attack to Upper-layer protocol by crafted ICMPv6 error messages,
RFC4942;RFC5927
4-3 Covert conversation through the payload of ICMPv6 error messages,
RFC4942
4-4 DoS attack by unprocessable packets to router,
RFC4942;RFC5927

5. IP Address definition

5-1 Anycast Traffic Identification,
RFC4942;RFC4291
5-2 Site Local Address as well-known DNS server addresses,
draft-ietf-ipngwg-dns-discovery-03;RFC6586
5-3 Malicious use of IPv6 addressing scheme,
RFC4942;RFC5157;draft-ietf-opsec-ipv6-host-scanning-04
5-4 Dynamic DNS and secure updates,

```
         RFC4942;RFC4472
     5-5 Complexity on plural address operating by IPv4-mapped address,
         RFC4942
     5-6 Filtering policy evasion using by IPv4-mapped address
         RFC4942
     5-7 Firewalls cannot perform deep packet inspection and filtering
         with IPSec,
         RFC4942
     5-8 IPv6 tunnels break IPv4 network security policy,
         RFC4942
   6. Multicast

     6-1 DoS attack by hijacked multicast router,
         RFC3810
     6-2 DoS attack by forged Report message in MLD,
         RFC3810;RFC2710
     6-3 Extra processing on the network equipment by forged Done
         messages in MLD,
         RFC3810;RFC2710
     6-4 DoS attack over multicast network with ICMPv6 error messages,
         RFC4942
     6-5 Abuse in multicast distribution tree on PIM-DM with
         temporary addresses,
         RFC3973
     6-6 Denial-of-Service Attack on the Link,
         RFC5294

   7. Mobile IPv6

     7-1 Attacks against Binding Update Protocols,
         RFC4225

     7-2 Filtering Policy evasion due to not support type 2 routing
         header,
         RFC4225;RFC6275

   8. Tunneling

     8-1 Filtering Policy evasion occurred in IPv6 transition/coexistence
         technologies on "IPv4-only" networks,
         RFC4942;RFC6169;RFC7123
     8-2 Source Routing after the Tunnel Client combined with old
         specification of Routing Header 0,
         RFC6169;RFC5095;RFC7123
     8-3 Attacks by malicious use of NDP may go to 6to4 Router/6to4
         Relay Router/6rd Border Router,
         RFC3964;RFC4942;RFC5969;RFC7123
     8-4 Attack toward IPv6 clients from IPv4 network via
```

6to4 Router/6to4 Relay Router,
RFC3964;RFC6169RFC5969;RFC7123

8-5 Attack toward 6to4 clients from IPv4 network via
6to4 Router/6to4 Relay Router,
RFC3964;RFC6169RFC5969;RFC7123

8-6 IPv4 broadcast attack via 6to4 Router/6to4 Relay Router,
RFC3964;RFC6169RFC5969;RFC7123

8-7 Sniffing at 6to4 Router/6to4 Relay Router,
RFC3964;RFC6169;RFC5969;RFC7123

8-8 Routing Loop Attack Using IPv6 Automatic Tunnels,
RFC6324

8-9 Filtering bypass by Teredo,
RFC6169;RFC7123

8-10 Port exposure with Teredo,
RFC6169;RFC5991;RFC7123

8-11 Teredo Tunnel Address Concerns,
RFC6119

8-12 Sniffing at Teredo Router/Teredo Relay Router,
RFC3964;RFC6169;RFC5969;RFC7123

9. Translation

9-1 Address Spoofing used by IPv4-embedded IPv6 address,
RFC6052;RFC6145;RFC6889

9-2 Concerns of using DNS64,
RFC6147;RFC6889

10. DNS

10-1 Dual stack operation bring overloading to name servers,
RFC4472;RFC4942;draft-ietf-dnsop-respsize-15

10-2 Operational difficulty of reverse zones and concerns,
RFC4472;RFC4942

10-3 Rogue DHCPv6 Servers,
draft-ietf-opsec-dhcpv6-shield-04

11. Other Operational concerns

11-1 Network segment violation by leakage of NDP in VLAN networks

11-2 RFC5952 text representation compliance for safer operation,
RFC5952

11-3 Dual stack nodes in IPv4 only network without supervision

Authors' Addresses

Masayuki Nakatani
Japan Computer Emergency Response Team Coordination Center
3-17, Kanda Nishiki-cho, Chiyoda-ku, Tokyo,
Japan

EMail: ww-info@jpcert.or.jp

Yoshiaki Kitaguchi
Kanazawa University
Kakuma-machi, Kanazawa, Ishikawa,
Japan

EMail: kitaguchi@imc.kanazawa-u.ac.jp

Kenichi Nagami
INTEC Inc.
1-3-3, Shinsuna, Koto-ku, Tokyo,
Japan

EMail: nagami@inetcore.com

Masataka Kosugi
INTEC Inc.
626-1, Kyoda, Takaoka-City, Toyama,
Japan

EMail: kosugi_masataka@intec.co.jp

Ruri Hiromi
INTEC Inc.
1-1-25, Shin Urashima-cho, Kanagawa-ku, Yokohama,
Japan

EMail: hiromi@inetcore.com