INTERNET-DRAFT
Intended Status: Informational
Expires: June 4, 2015

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

December 1, 2014

Introducing IPv6 vulnerability test program in Japan
draft-jpcert-ipv6vullnerability-check-02

Abstract

Japan Computer Emergency Response Team Coordination Center, known as JPCERT/CC have been researching about vulnerability in use of IPv6. JPCERT/CC provided the information toward vendors in Japan. They also verified the occurring those security incidents 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 experiment of activity.

Status of this Memo

This Internet-Draft is submitted to IETF in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/1id-abstracts.html

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html

Copyright and License Notice

Copyright (c) 2014 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (http://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

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 this 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

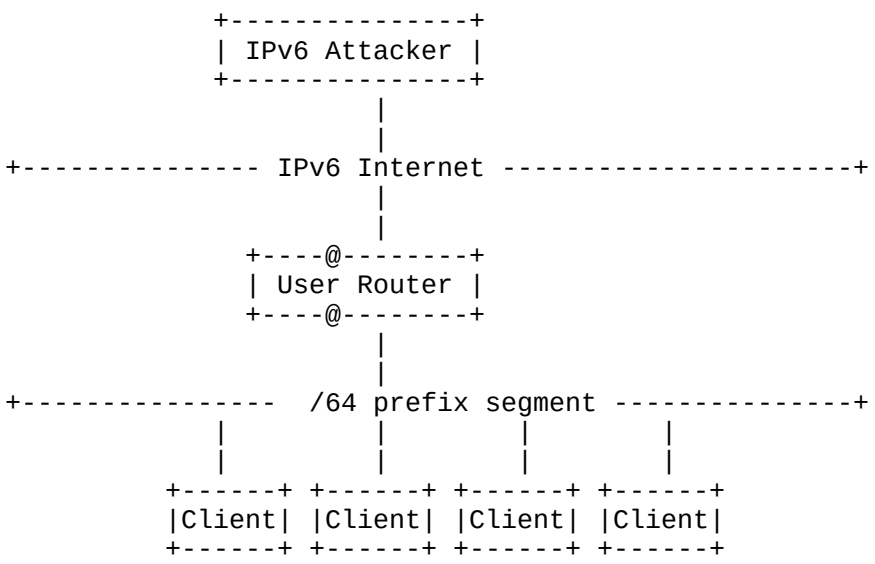
The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

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



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 tests 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

[RFC1858] G. Ziemba, D. Reed, and P. Traina, "Security Considerations for IP Fragment Filtering", RFC 1858, October 1995.

[RFC1883] S. Deering, and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification (Obsoleted by RFC 2460)", RFC 1883, December 1995.

[RFC2460] S. Deering, and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", RFC 2460, December 1998.

[RFC2529] B. Carpenter and C. Jung, "Transmission of IPv6 over IPv4 Domains without Explicit Tunnels", RFC 2529, March 1999.

[RFC2661] W. Townsley, A. Valencia, A. Rubens, G. Pall, G. Zorn and B. Palter, "Layer Two Tunneling Protocol "L2TP"", RFC 2661, August 1999.

[RFC2671] P. Vixie, "Extension Mechanisms for DNS (EDNS0)", RFC 2661, August 1999.

[RFC2675] D. Borman, S. Deering and R. Hinden "IPv6 Jumbograms", RFC 2675, August 1999.

[RFC2694] P. Srisuresh, G. Tsirtsis, P. Akkiraju and A. Heffernan, "DNS extensions to Network Address Translators (DNS_ALG)", RFC 2694, September 1999.

[RFC2710] S. Deering, W. Fenner and B. Haberman, "Multicast Listener Discovery (MLD) for IPv6", RFC 2710, October 1999.

[RFC2766] G. Tsirtsis and P. Srisuresh, "Network Address Translation - Protocol Translation (NAT-PT)", RFC 2766, February 2000.

[RFC3056] B. Carpenter and K. Moore, "Connection of IPv6 Domains via IPv4 Clouds", RFC 3056, February 2001.

[RFC3068] C. Huitema, "An Anycast Prefix for 6to4 Relay Routers", RFC 3068, June 2001.

[RFC3089] H. Kitamura, "A SOCKS-based IPv6/IPv4 Gateway Mechanism", RFC 3089, April 2001.

[RFC3128] I. Miller, "Protection Against a Variant of the Tiny

Fragment Attack", RFC 3128, June 2001.

[RFC3142] J. Hagino and K. Yamamoto, "An IPv6-to-IPv4 Transport Relay Translator", RFC 3142, June 2001.

[RFC3493] R. Gilligan, S. Thomson, J. Bound, J. McCann and W. Stevens, "Basic Socket Interface Extensions for IPv6", RFC 3493, February 2003.

[RFC3756] P. Nikander, J. Kempf and E. Nordmark, "IPv6 Neighbor Discovery (ND) Trust Models and Threats", RFC 3756, May 2004.

[RFC3775] Johnson, D., Perkins, C. and J. Arkko, "Mobility Support in IPv6", RFC 3775, June 2004.

[RFC3810] R. Vida and L. Costa, "Multicast Listener Discovery Version 2 (MLDv2) for IPv6", RFC 3810, June 2004.

[RFC3879] C. Huitema and B. Carpenter, "Deprecating Site Local Addresses", RFC 3879, September 2004.

[RFC3964] P. Savola and C. Patel, "Security Considerations for 6to4", RFC 3964, December 2004.

[RFC3971] J. Arkko, J. Kempf, B. Zill and P. Nikander, "SEcure Neighbor Discovery (SEND)", RFC 3971, March 2005.

[RFC3972] T. Aura, "Cryptographically Generated Addresses (CGA)", RFC 3972, March 2005.

[RFC3973] A. Adams, J. Nicholas and W. Siadak, "Protocol Independent Multicast - Dense Mode (PIM-DM): Protocol Specification (Revised)", RFC 3973, January 2005.

[RFC4191] R. Draves and D. Thaler, "Default Router Preferences and More-Specific Routes", RFC 4191, November 2005.

[RFC4193] R. Hinden and B. Haberman, "Unique Local IPv6 Addresses", RFC 4193, October 2005.

[RFC4225] P. Nikander, J. Arkko, T. Aura, G. Montenegro and E. Nordmark, "Mobile IP Version 6 Route Optimization Security Design Background", RFC 4225, December 2005.

[RFC4291] R. Hinden and S. Deering, "IP Version 6 Addressing Architecture", RFC 4291, February 2006.

[RFC4380] C. Huitema, "Teredo: Tunneling IPv6 over UDP through Network Address Translations (NATs)", RFC 4380, February 2006.

[RFC4795] B. Aboba, D. Thaler and L. Esibov, "Link-Local Multicast Name Resolution (LLMNR)", RFC 4795, January 2007.

[RFC4861] T. Narten, E. Nordmark, W. Simpson and H. Soliman, "Neighbor Discovery for IP Version 6 (IPv6)", RFC 4861, September 2007.

[RFC4862] S. Thomson, T. Narten and T. Jinmei, "IPv6 Stateless Address Autoconfiguration", RFC 4862, September 2007.

[RFC4941] Narten, T., Draves, R., and S. Krishnan, "Privacy Extensions ‘for Stateless Address Autoconfiguration in IPv6", RFC 4941, September 2007.

[RFC4942] E. Davies, S. Krishnan and P. Savola, "IPv6 Transition/Co-existence Security Considerations", RFC 4942, September 2007.

[RFC4943] S. Roy, A. Durand and J. Paugh, "IPv6 Neighbor Discovery On-Link Assumption Considered Harmful", RFC 4943, September 2007.

[RFC4966] C. Aoun and E. Davies, "Reasons to Move the Network Address Translator - Protocol Translator (NAT-PT) to Historic Status", RFC 4966, July 2007.

[RFC5095] C. Malamud, "Deprecation of Type 0 Routing Headers in IPv6", RFC 5095, May 2005.

[RFC5110] P. Savola, "Overview of the Internet Multicast Routing Architecture", RFC 5110, January 2008.

[RFC5157] T. Chown, "IPv6 Implication for Network Scanning", RFC 5157, March 2008.

[RFC5214] Templin, F., Gleeson T., and D. Thaler, "Intra-Site Automatic Tunnel Addressing Protocol (ISATAP)", RFC 5214, March 2008.

[RFC5227] S. Cheshire, "IPv4 Address Conflict Detection", RFC 5227, July 2008.

[RFC5294] P. Savola and J. Lingard, "Host Threats to Protocol Independent Multicast (PIM)", RFC 5294, August 2008.

[RFC5572] M. Blanchet and F. Parent, "IPv6 Tunnel Broker with the Tunnel Setup Protocol (TSP)", RFC 5572, February 2010.

[RFC5722] S. Krishnan, "Handling of Overlapping IPv6 Fragments", RFC 5722, December 2009.

[RFC5927] F. Gont, "ICMP Attacks against TCP", RFC 5927, July 2010.

[RFC5952] S. Kawamura and M. Kawashima, "A Recommendation for IPv6 Address Text Representation", RFC 5952, August 2010.

[RFC5969] W. Townsley and O. Troan, "IPv6 Rapid Deployment on IPv4 Infrastructures (6rd) -- Protocol Specification", RFC 5969, August 2010.

[RFC5991] D. Thaler, S. Krishnan and J. Hoagland, "Teredo Security Updates", RFC 5991, September 2010.

[RFC6052] C. Bao, C. Huitema, M. Bagnulo, M. Boucadair and X. Li, "IPv6 Addressing of IPv4/IPv6 Translators", RFC 6052, October 2010.

[RFC6104] T. Chown and S. Venaas, "Rogue IPv6 Router Advertisement Problem Statement", RFC 6104, February 2011.

[RFC6105] E. Levy-Abegnoli, G. Van de Velde, C. Popoviciu and J. Mohacsi, "IPv6 Router Advertisement Guard", RFC 6105, February 2011.

[RFC6106] J. Jeong, S. Park, L. Beloeil and S. Madanapalli, "IPv6 Router Advertisement Options for DNS Configuration", RFC 6106, November 2010.

[RFC6144] F. Baker, X. Li, C. Bao and K. Yin, "Framework for IPv4/IPv6 Translation", RFC 6144, April 2011.

[RFC6145] X. Li, C. Bao and F. Baker, "IP/ICMP Translation Algorithm", RFC 6145, April 2011.

[RFC6146] M. Bagnulo, P. Matthews and I. Beijnum, "Stateful NAT64: Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers", RFC 6146, April 2011.

[RFC6147] M. Bagnulo, A. Sullivan, P. Matthews and I. Beijnum, "DNS64: DNS Extensions for Network Address Translation from IPv6 Clients to IPv4 Servers", RFC 6147, April 2011.

[RFC6169] S. Krishnan, D. Thaler and J. Hoagland, "Security Concerns

with IP Tunneling", RFC 6169, April 2011.

[RFC6275] C. Perkins, D. Johnson and J. Arkko, "Mobility Support in IPv6", RFC 6275, July 2011.

[RFC6296] M. Wasserman and F. Baker, "IPv6-to-IPv6 Network Prefix Translation", RFC 6296, June 2011.

[RFC6324] G. Nakibly and F. Templin, "Routing Loop Attack Using IPv6 Automatic Tunnels: Problem Statement and Proposed Mitigations", RFC 6324, August 2011.

[RFC6437] S. Amante, B. Carpenter, S. Jiang and J. Rajahalme, "IPv6 Flow Label Specification", RFC 6437, November 2011.

[RFC6564] S. Krishnan, J. Woodyatt, E. Kline, J. Hoagland and M. Bhatia, "A Uniform Format for IPv6 Extension Headers", RFC 6564, April 2012.

[RFC6583] I. Gashinsky, J. Jaeggli and W. Kumari, "Operational Neighbor Discovery Problems", RFC 6583, March 2012.

[RFC6586] J. Arkko and A. Keranan, "Experiences from an IPv6-Only Network", RFC 6586, April 2012.

[ID-dns-discovery] D. Thaler and J. Hagino, "IPv6 Stateless DNS Discovery ", draft-ietf-ipngwg-dns-discovery-03, November 2001. (expired)

[ID-ipv6-hopbyhop] S. Krishnan, "The case against Hop-by-Hop options", draft-krishnan-ipv6-hopbyhop-05, October 2010. (expired)

[RFC6762] S. Cheshire and M. Krochmal, "Multicast DNS", RFC 6762, February 2013.

[RFC6763] S. Cheshire and M. Krochmal, "DNS-Based Service Discovery", RFC 6763, February 2013.

[ID-ipv6-smurf-amplifier] F. Gont, "Security Implications of IPv6 options of Type 10xxxxxx", draft-gont-6man-ipv6-smurf-amplifier-02, March 2013. (expired)

[ID-tiny-fragments-issues] V. Manral, "Tiny Fragments in IPv6", draft-manral-6man-tiny-fragments-issues-00, February 2012. (expired)

[ID-predictable-fragment-id] F. Gont, "Security Implications of

Predictable Fragment Identification Values", draft-ietf-6man-predictable-fragment-id-01, April 2014.

[ID-flowlabel-security] F. Gont, "Security Assessment of the IPv6 Flow Label", draft- gont-6man-flowlabel-security-03, March 2012. (expired)

[RFC6889] R. Renno, T. Saxena, M. Boucadair and S. Sivakumar, "Analysis of Stateful 64 Translation", RFC 6889, April 2013.

[ID-dnsop-respsize] P. Vixie and A. Kato, "DNS Referral Response Size Issues", draft-ietf-dnsop-respsize-15, February 2014.

[RFC7112] F. Gont and V. Manral, "Implications of Oversized IPv6 Header Chains", RFC 7112, January 2014.

[ID-slaac-dns-config-issues] F. Gont and P. Simerda, "Current issues with DNS Configuration Options for SLAAC", draft-gont-6man-slaac-dns-config-issues-00, June 2012. (expired)

[ID-dhcpv6-sheald] F. Gont, W. Liu and G. Van de Velde, "DHCPv6-Shield: Protecting Against Rogue DHCPv6 Servers", draft-ietf-opsec-dhcpv6-shield-04, July 2014.

[RFC7113] F. Gont, "Implementation Advice for IPv6 Router Advertisement Guard (RA-Guard)", RFC 7113, February 2014.

[RFC6946] F. Gont, "Processing of IPv6 "atomic" fragments", RFC 6046, May 2013.

[RFC6980] F. Gont, "Security Implications of IPv6 Fragmentation with IPv6 Neighbor Discovery", RFC 6980, August 2013.

[RFC7123] F. Gont and W. Liu, "Security Implications of IPv6 on IPv4 Networks", RFC 7123, February 2014.

[ID-ipv6-host-scanning] F. Gont and T. Chown, "Network Reconnaissance in IPv6 Networks", draft-ietf-opsec-ipv6-host-scanning-04, June 2014.

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