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

K.Shikano
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-00

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.

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

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 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

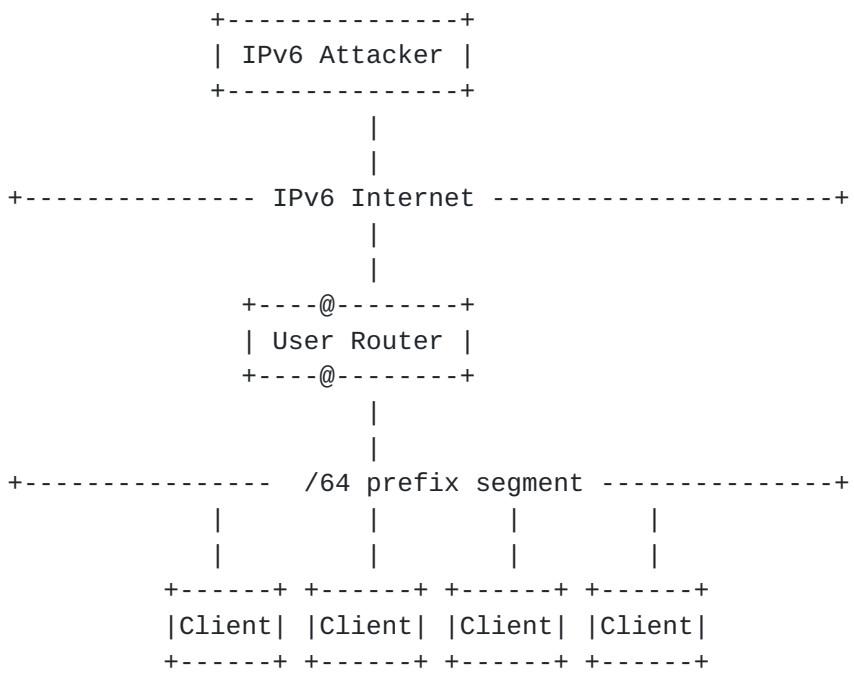
The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

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



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	comply the DoS resistance policy(*)
	packet filtering evasion	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. 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

TBD

Authors' Addresses

Shikano Keisuke
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-cho, Kanazawa-City, Ishikawa,
Japan

EMail: name@example.com

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