Header of death: security implications of IPv6 extension headers to the open-source firewall

Anazel P. Gamilla, Marlon A. Naagas
Department of Information Technology, Central Luzon State University, Science City of Munoz, Nueva Ecija, Philippines

Article Info

Article history:

Received Oct 15, 2021
Revised Dec 16, 2021
Accepted Jan 16, 2022

Keywords:

IPv6 denial of service
IPv6 extension headers
IPv6 open-source firewall
IPv6 protocol
IPv6 security threats

ABSTRACT

IPv6 extension headers (EHs) contain additional information utilized by network devices (such as routers and firewalls) to determine how to direct or process an IPv6 packet. However, the use of excessive and unknown EHs can lead to the security implications such as evasion and denial of service (DoS) of the target firewall. Study revealed that there is no permanent remediation that prevents the IPv6 EHs attack from invading the open-source firewalls by default. Using IPv6 packet manipulations technique, the attacker can evade the target network including the firewall and target host that can lead to a complete unavailability of network service. The common vulnerability scoring system (CVSS) also indicates that the base, temporal, and environment metric groups of IPv6 EHs vulnerabilities were in the critical level of severity. Quick and dirty solutions such as denying and allowing packets and IP addresses as preventive measures is still one of the effective ways of defending against the EHs packet manipulation attacks, as a temporary solution to date.

Corresponding Author:

Marlon A. Naagas
Department of Information Technology College of Engineering, Central Luzon State University
Science City of Munoz, Nueva Ecija, Philippines
Email: manaagas@clsu.edu.ph

1. INTRODUCTION

The first COVID-19 outbreak was detected between late 2019 in Wuhan China, the pandemic has had an enormous impact on people’s lives and society. Most affected countries are facing an extraordinary health crisis that has a great impact on their economic and social structures for a long time. Society urges us to respect lockdown and social distancing to limit the spreading of infection. However, shifting to online sessions and adopting flexible workplace solutions are the best solution so far seen by the government to limit the people's movement and to continue to live into the new normal [1]. One of the interesting impacts of the pandemic has been its influence on the internet, and this effect can be observed in the historical IPv6 traffic volume measurements [2]. As reported by Asia pacific network information centre APNIC, the distribution of IPv6 has expanded from 15% in 2018 to 20% this year, but security issues have become the number one challenge. Denial of service (DoS) attacks, phishing, spam, ransomware, and malware remain the biggest network security issues faced. Forty-one percent (41%) of respondents indicated that DoS attacks are one of the main network security threats that their organization faces [3].

The implementation of IPv6 offers major improvements in the development of the new protocol which includes the extension headers (EHs) [4]. EHs provide supplementary information that will help network devices like routers, switches, and end-devices to decide how to direct or process an IPv6 packet along the network [5]. However, many threats that are associated with EHs have been discovered and it is used by the threat actor as a new attack vector nowadays. As an early adapter, preparing what will be the security measures to prevent the emerging threats of IPv6 from the time of deployment. As a security measure, the most typical way to secure the network is by implementing a firewall as the first line of defense [6]. Firewall imposes security policies using ingress/egress packet filtering. Firewalls generally inspect network layer and transport layer traffic but can often assess the traffic flows of the application layer. However, processing of IPv6 EHs become a huge challenge to a network firewall, because: EHs are not “processed, inserted, or deleted by any node along a packet's delivery path until the packet reaches the node identified in the destination address field of the IPv6 header” [4], this kind of characteristics, with proper packet exploitation will lead to the evasion at the IP level. The attacker will use these characteristics to hide the attack by manipulating IPv6 packets by inserting an EHs chain payloads to create a covert channel. Validating the contents of the packets through EHs manipulation can waste CPU resources and possibly perform a DoS. While, the security implications of the fragment header packet manipulation, based on flooding a target with IPv6 fragments could be subject to DoS attack to information leakage attacks [7]. The massive increase of such unknown EHs can decrease the firewall's capabilities to process Layer 4 information [8]. Moreover, the evasion of security controls, DoS in line with processing requirements, and DoS in line with implementation errors are some of the security implications produced by mishandling of IPv6 EHs [9].

Several pieces of research publications have shown that most of the popular firewalls today were vulnerable to EHs manipulation [10]-[12]. A number of firewalls still cannot handle IPv6 traffic or it has limited abilities to filter IPv6 traffic but still, some can filter IPv6 traffic to approximately the same extent as IPv4 traffic [13]. Many widely used stateful firewalls do not support IPv6 at all, or the implementations are lacking. Some later implementations have not yet been tested in the network environments of organizations. Due to the problems during the deployment stage of stateful filtering, some organizations have ended up implementing stateless filtering for IPv6 traffic [14], [15].

The goal of this paper is to provide clarity and revisit if the firewalls today are capable of handling IPv6-related attacks in general, particularly EHs packet manipulation attacks. The study will assess the impact of IPv6 EHs packet manipulations threats to two of the most popular open-source NIDS/NIPS firewalls. The result of this study will also expose the limitations of the chosen firewalls and recommended solutions on how to mitigate the attacks. This research is the continuation of our IPv6 EHs security research series.

2. METHOD

2.1. Experimental set-up

This study was conducted at Central Luzon State University Network–network operation center (NOC). Two popular stateful firewalls were also deployed and evaluated, see Figure 1. For the reason of convenience, snort and suricata were installed in the Pfsense platform because it is one of the popular open-source firewall routers especially in the Philippines and it has built-in stateful firewall functionality. Emerging threats and snort community rules were uploaded on both firewalls as a default ruleset for the two firewalls. The research methods were crafted using 2 systematic approaches that combine with the practical vulnerability analysis/penetration testing of VAPT approach and common vulnerability scoring system (CVSS) analysis for the risk assessment.

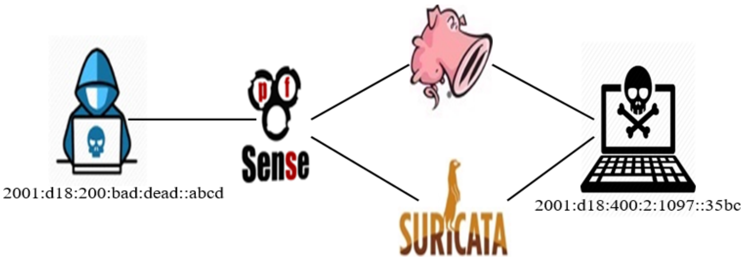
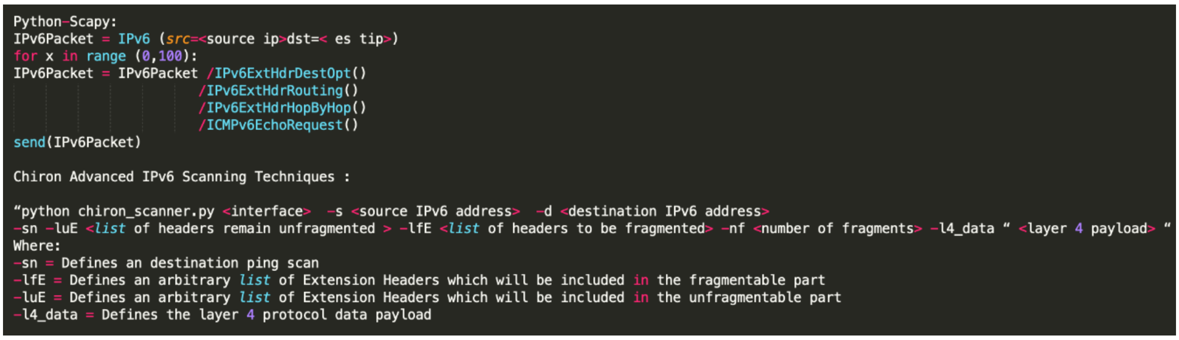


Figure 1. Experimental setup

The attacker's goal is to send layer 4 payloads alongside ping6 and get a reply back from a target without being detected by the IDS. The penetration testing was performed on the existing network configuration of the host university, the security tests were performed after office hours to assure that no network disruptions happened during the experiment. To carry out the process of VAPT, the researcher established an actual network in which will provide an environment for the analysis of network behaviour during the new security model designing and development. For the IPv6 EHs attack vectors, twelve (12) malformed packets are used and crafted to test the security performance of the chosen firewalls during the evasion attacks in Table 1. Python-Scapy and Chiron are the scripting tools used in developing IPv6 packets. Figure 2 presents the sample script of a rouge packet with multiple EHs. Most of the attack vectors used in this study were adopted to [10] since this study is a continuation of the IPv6 EHs security research series.

Table 1. IPv6 EHs attack vectors

Test Id	Attack vectors
EH.A1	Hop-By-Hop extension header with multiple large arbitrary payload in PadN option data at the IP level-covert channel
EH.A2	Hop-By-Hop extension header mixing with multiple fragmentation header and destination header with large arbitrary data at the IP level covert channel
EH.A3	Destination options extension header with multiple large arbitrary payload in PadN option data at the IP level-covert channel
EH.A4	Mixing of multiple fragmentation header and destination header with large arbitrary payload at the IP level-covert channel
EH.A5	Mixing multiple and various EHs per datagram in atomic fragments
EH.A6	Mixing of multiple EHs at the 1st fragment combining with upper-layer protocol header at the 2nd fragment
EH.A7	Mixing of different EHs in fragment and unfragment part with a layer 4 payload
EH.A8	Fragmentation overlapping using Paxson/Shankar model
EH.A9	Router alert within the hop-by-hop options header
EH.A10	Router alert within fragmentation and ehs in both the fragmentable and the unfragmentable part.
EH.A11	Type-0 Routing header (RH0)-CISCO model
EH.A12	Type-0 Routing header within hop-by-hop extension header and a fragmented destination options header.



```
Python-Scapy:
IPv6Packet = IPv6 (src=<source ip>dst=< es tip>)
for x in range (0,100):
IPv6Packet = IPv6Packet /IPv6ExtHdrDestOpt()
                       /IPv6ExtHdrRouting()
                       /IPv6ExtHdrHopByHop()
                       /ICMPv6EchoRequest()
send(IPv6Packet)

Chiron Advanced IPv6 Scanning Techniques :

“python chiron_scanner.py <interface>  -s <source IPv6 address>  -d <destination IPv6 address>
-sn -luE <list of headers remain unfragmented > -lfE <list of headers to be fragmented> -nf <number of fragments> -l4_data “ <layer 4 payload> “
Where:
-sn = Defines an destination ping scan
-lfE = Defines an arbitrary list of Extension Headers which will be included in the fragmentable part
-luE = Defines an arbitrary list of Extension Headers which will be included in the unfragmentable part
-l4_data = Defines the layer 4 protocol data payload
```

Figure 2. Sample script

2.2. Packet analysis

Active measurements were performed on the victim link, observing to which and how EHs are actually used by the attacker. The captured packets will be examined and extracted using the protocol analyzer tool wireshark. The captured packets will be used as evidence that even to this day, this EHs will be used as attack vectors to create a DoS and become a potential threat that the networking society needs to consider in their future IPv6 implementations.

3. RESULTS AND DISCUSSION

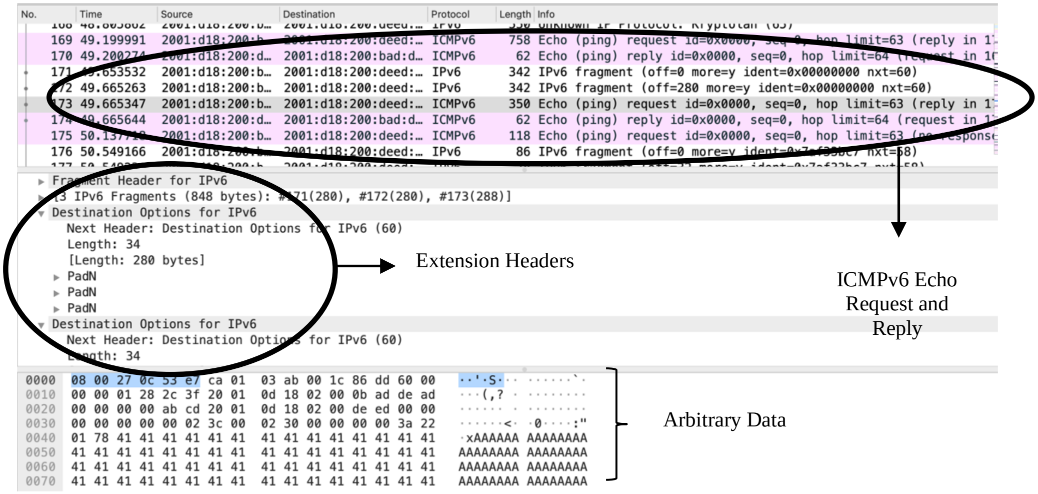
3.1. Firewall evasion

The main functionality of network intrusion detection systems (NIDS) is to analyze, detect and evaluate the traffic patterns that might be associated with network-based attacks. This middle-box system generally attempts to inspect both application-layer traffic (if possible) and layer 4 traffic flows but, at the bare minimum [16]. When an attack activity happens, it alerts the administrator for potential intrusion attempts. Similarly, the network intrusion prevention systems (NIPS) also works like NIDS but it also prevents intrusions by reacting to detected attack attempts by triggering packet filtering policies at firewalls and other devices [17].

Table 2 presents the complete list of firewall vulnerability tests against IPv6 EHs attack vectors. The overall result shows that nine out of twelve (9/12) attacks successfully evaded the firewalls, see Table 2. Figure 3 shows the network behavior of two firewalls was flooded by malformed packets performed by the attacker. The researchers combine different variations of hop-by-hop extension header, destination options extension header, fragmentation with multiple large arbitrary payloads in PadN option data at the IP Level to form a covert channel attack (EH.A1-EH.A4). As a result, the firewalls were tested vulnerable in this kind of attack until today. Results also show that four of the IP fragmentation attacks successfully landed on the target firewalls (EH.A5-EH.A6). One of the green lights on the chosen firewalls, the router alert, and router header 0 (RH0) were not viable today. The two firewalls reject the packets containing the Router Alert and RH0 (EH.A9, EH.A11, EH.A12). However, combining or hiding the router alert within fragmentation and EHs in both the fragmentable and the unfragmentable part of the IPv6 packet, the attack becomes successful (EH.A10).

Table 2. Complete list of firewall tests summary

Test Id	SNORT		SURICATA	
	Results	Remarks	Results	Remarks
EH.A1	With ICMPv6 echo request and reply	No alert	With ICMPv6 echo request and reply	With alert
EH.A2	With ICMPv6 echo request and reply	No alert	With ICMPv6 echo request and reply	With alert
EH.A3	With ICMPv6 echo request and reply	No alert	With ICMPv6 echo request and reply	With alert
EH.A4	With ICMPv6 echo request and reply	No alert	With ICMPv6 echo request and reply	With alert
EH.A5	With ICMPv6 echo request and reply	No alert	With ICMPv6 echo request and reply	With alert
EH.A6	With ICMPv6 echo request and reply	No alert	With ICMPv6 echo request and reply	With alert
EH.A7	With ICMPv6 echo request and reply	No alert	With ICMPv6 echo request and reply	With alert
EH.A8	With ICMPv6 echo request and reply	No alert	With ICMPv6 echo request and reply	With alert
EH.A9	No router alert received	No alert	No router alert received	With alert
EH.A10	With ICMPv6 echo request and reply	No alert	With ICMPv6 echo request and reply	No alert
EH.A11	No RH0 received	No alert	No RH0 received	No alert
EH.A12	No RH0 received	No alert	No RH0 received	No alert

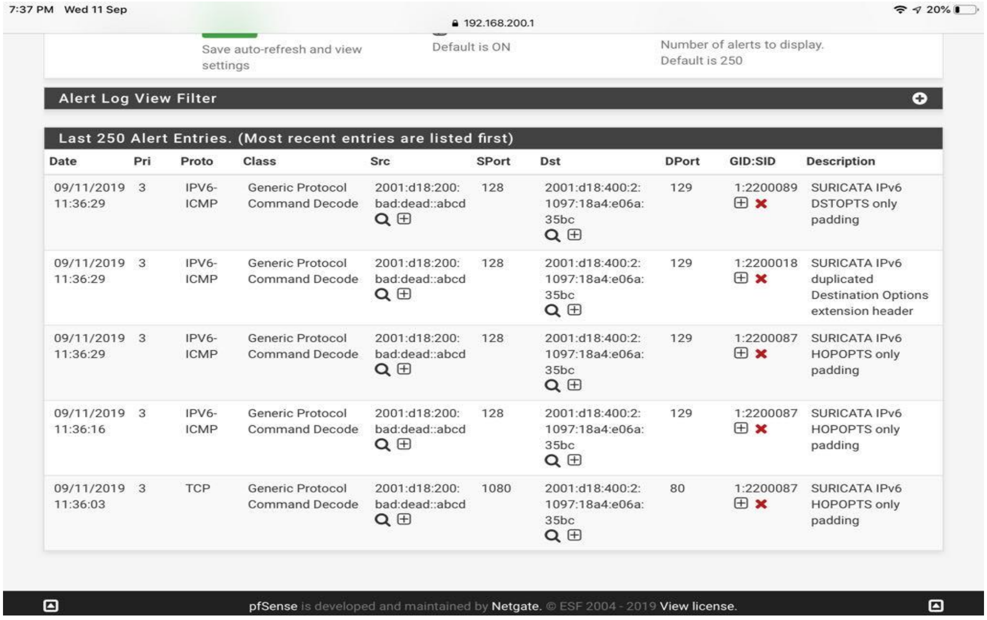


```
No.  Time       Source              Destination          Protocol  Length Info
169 49.199991  2001:d18:200:b…    2001:d18:200:deed:…  ICMPv6    758 Echo (ping) request id=0x0000, seq=0, hop limit=63 (reply in 1
170 49.200274  2001:d18:200:d…    2001:d18:200:bad:d…  ICMPv6     62 Echo (ping) reply id=0x0000, seq=0, hop limit=64 (request in 1
171 49.653532  2001:d18:200:b…    2001:d18:200:deed:…  IPv6      342 IPv6 fragment (off=0 more=y ident=0x00000000 nxt=60)
172 49.665263  2001:d18:200:b…    2001:d18:200:deed:…  IPv6      342 IPv6 fragment (off=280 more=y ident=0x00000000 nxt=60)
173 49.665347  2001:d18:200:b…    2001:d18:200:deed:…  ICMPv6    350 Echo (ping) request id=0x0000, seq=0, hop limit=63 (reply in 1
174 49.665644  2001:d18:200:d…    2001:d18:200:bad:d…  ICMPv6     62 Echo (ping) reply id=0x0000, seq=0, hop limit=64 (request in 1
175 50.1377    2001:d18:200:b…    2001:d18:200:deed:…  ICMPv6    118 Echo (ping) request id=0x0000, seq=0, hop limit=63 (no respons
176 50.549166  2001:d18:200:b…    2001:d18:200:deed:…  IPv6       86 IPv6 fragment (off=0 more=y ident=0x7af33bc7 nxt=58)

▸ Fragment Header for IPv6
▸ [3 IPv6 Fragments (848 bytes): #171(280), #172(280), #173(288)]
▾ Destination Options for IPv6
    Next Header: Destination Options for IPv6 (60)
    Length: 34
    [Length: 280 bytes]
  ▸ PadN
  ▸ PadN
  ▸ PadN
▾ Destination Options for IPv6
    Next Header: Destination Options for IPv6 (60)
    Length: 34

0000  08 00 27 0c 53 e7 ca 01  03 ab 00 1c 86 dd 60 00   ··'·S··· ······`·
0010  00 00 01 28 2c 3f 20 01  0d 18 02 00 0b ad de ad   ···(,? · ········
0020  00 00 00 00 ab cd 20 01  0d 18 02 00 de ed 00 00   ······ · ········
0030  00 00 00 00 00 02 3c 00  02 30 00 00 00 00 3a 22   ······<· ·0····:"
0040  01 78 41 41 41 41 41 41  41 41 41 41 41 41 41 41   ·xAAAAAA AAAAAAAA
0050  41 41 41 41 41 41 41 41  41 41 41 41 41 41 41 41   AAAAAAAA AAAAAAAA
0060  41 41 41 41 41 41 41 41  41 41 41 41 41 41 41 41   AAAAAAAA AAAAAAAA
0070  41 41 41 41 41 41 41 41  41 41 41 41 41 41 41 41   AAAAAAAA AAAAAAAA
```

Figure 3. Network behavior during attacks

Moreover, the tests revealed that snort did not issue any single alert, see Table 2 (Snort), while Suricata generated an alert to the user while performing a security evasion, see Table 2 (Suricata) and Figure 4. In this case, Suricata performed much better against Snort in terms of alerting the users about the EHs attacks. However, even though Suricata produced an alert to the users, the tests also revealed that the victim OS is still receiving attacker payload, see Figure 5, the firewalls didn't do anything to reject or stop the malformed packet in penetrating the network by default.

Further, results also showed that the NIDS/NIPS (open-source) obtained false-positive or false-negative findings. In this case, the NIDS/NIPS provide the administrator a wrong signal that affects the way to organize, tune and understand relevant network audit trails and other logs that are otherwise difficult to track or parse [18]. False-positive and false-negative are NIDS/NIPS serious mistakes because it misses the threats and allows a large number of illegitimate payloads to enter the network. The administrator has no idea that the attack is in place until they discover that the network has been affected and exhausted.



7:37 PM Wed 11 Sep

192.168.200.1

20%

Save auto-refresh and view settings

Default is ON

Number of alerts to display. Default is 250

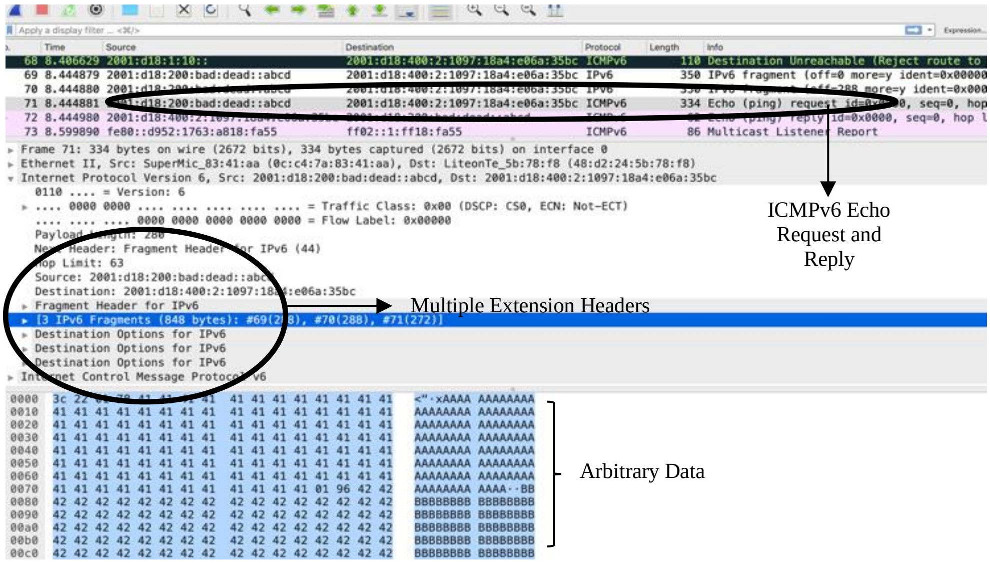
Alert Log View Filter

Last 250 Alert Entries. (Most recent entries are listed first)

Date	Pri	Proto	Class	Src	SPort	Dst	DPort	GID:SID	Description
09/11/2019 11:36:29	3	IPV6-ICMP	Generic Protocol Command Decode	2001:d18:200:bad:dead::abcd	128	2001:d18:400:2:1097:18a4:e06a:35bc	129	1:2200089	SURICATA IPv6 DSTOPTS only padding
09/11/2019 11:36:29	3	IPV6-ICMP	Generic Protocol Command Decode	2001:d18:200:bad:dead::abcd	128	2001:d18:400:2:1097:18a4:e06a:35bc	129	1:2200018	SURICATA IPv6 duplicated Destination Options extension header
09/11/2019 11:36:29	3	IPV6-ICMP	Generic Protocol Command Decode	2001:d18:200:bad:dead::abcd	128	2001:d18:400:2:1097:18a4:e06a:35bc	129	1:2200087	SURICATA IPv6 HOPOPTS only padding
09/11/2019 11:36:16	3	IPV6-ICMP	Generic Protocol Command Decode	2001:d18:200:bad:dead::abcd	128	2001:d18:400:2:1097:18a4:e06a:35bc	129	1:2200087	SURICATA IPv6 HOPOPTS only padding
09/11/2019 11:36:03	3	TCP	Generic Protocol Command Decode	2001:d18:200:bad:dead::abcd	1080	2001:d18:400:2:1097:18a4:e06a:35bc	80	1:2200087	SURICATA IPv6 HOPOPTS only padding

pfSense is developed and maintained by Netgate. © ESF 2004 - 2019 View license.

Figure 4. Suricata alert during attacks



```
Apply a display filter ... <⌘/>
No.  Time      Source                          Destination                         Protocol  Length  Info
  68 8.406629  2001:d18:1:10::                 2001:d18:400:2:1097:18a4:e06a:35bc  ICMPv6    110 Destination Unreachable (Reject route to
  69 8.444879  2001:d18:200:bad:dead::abcd     2001:d18:400:2:1097:18a4:e06a:35bc  IPv6      350 IPv6 fragment (off=0 more=y ident=0x00000
  70 8.444880  2001:d18:200:bad:dead::abcd     2001:d18:400:2:1097:18a4:e06a:35bc  IPv6      350 IPv6 fragment (off=288 more=y ident=0x000
  71 8.444881  2001:d18:200:bad:dead::abcd     2001:d18:400:2:1097:18a4:e06a:35bc  ICMPv6    334 Echo (ping) request id=0x0000, seq=0, hop
  72 8.444980  2001:d18:400:2:1097:18a4:e06a:35bc 2001:d18:200:bad:dead::abcd      ICMPv6     62 Echo (ping) reply id=0x0000, seq=0, hop l
  73 8.599890  fe80::d952:1763:a818:fa55       ff02::1:ff18:fa55                   ICMPv6     86 Multicast Listener Report
▸ Frame 71: 334 bytes on wire (2672 bits), 334 bytes captured (2672 bits) on interface 0
▸ Ethernet II, Src: SuperMic_83:41:aa (0c:c4:7a:83:41:aa), Dst: LiteonTe_5b:78:f8 (48:d2:24:5b:78:f8)
▾ Internet Protocol Version 6, Src: 2001:d18:200:bad:dead::abcd, Dst: 2001:d18:400:2:1097:18a4:e06a:35bc
    0110 .... = Version: 6
  ▸ .... 0000 0000 .... .... .... .... .... = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)
    .... .... .... 0000 0000 0000 0000 0000 = Flow Label: 0x00000
    Payload Length: 280
    Next Header: Fragment Header for IPv6 (44)
    Hop Limit: 63
    Source: 2001:d18:200:bad:dead::abcd
    Destination: 2001:d18:400:2:1097:18a4:e06a:35bc
  ▸ Fragment Header for IPv6
  ▸ [3 IPv6 Fragments (848 bytes): #69(288), #70(288), #71(272)]
  ▸ Destination Options for IPv6
  ▸ Destination Options for IPv6
  ▸ Destination Options for IPv6
▸ Internet Control Message Protocol v6
0000  3c 22 01 78 41 41 41 41  41 41 41 41 41 41 41 41   <"·xAAAA AAAAAAAA
0010  41 41 41 41 41 41 41 41  41 41 41 41 41 41 41 41   AAAAAAAA AAAAAAAA
0020  41 41 41 41 41 41 41 41  41 41 41 41 41 41 41 41   AAAAAAAA AAAAAAAA
0030  41 41 41 41 41 41 41 41  41 41 41 41 41 41 41 41   AAAAAAAA AAAAAAAA
0040  41 41 41 41 41 41 41 41  41 41 41 41 41 41 41 41   AAAAAAAA AAAAAAAA
0050  41 41 41 41 41 41 41 41  41 41 41 41 41 41 41 41   AAAAAAAA AAAAAAAA
0060  41 41 41 41 41 41 41 41  41 41 41 41 41 41 41 41   AAAAAAAA AAAAAAAA
0070  41 41 41 41 41 41 41 41  41 41 41 41 01 96 42 42   AAAAAAAA AAAA··BB
0080  42 42 42 42 42 42 42 42  42 42 42 42 42 42 42 42   BBBBBBBB BBBBBBBB
0090  42 42 42 42 42 42 42 42  42 42 42 42 42 42 42 42   BBBBBBBB BBBBBBBB
00a0  42 42 42 42 42 42 42 42  42 42 42 42 42 42 42 42   BBBBBBBB BBBBBBBB
00b0  42 42 42 42 42 42 42 42  42 42 42 42 42 42 42 42   BBBBBBBB BBBBBBBB
00c0  42 42 42 42 42 42 42 42  42 42 42 42 42 42 42 42   BBBBBBBB BBBBBBBB
```

Figure 5. Suricata sample packet capture with attacker payload

3.2. Impact of IPv6 extension headers to open-source firewall

The researchers utilized the common vulnerability scoring system version 3.1 (CVSSv3.1), an open industry standard to assess the severity of computer system security vulnerabilities which includes the scoring of three metrics groups, the based, the temporal, and the environmental metrics and each of them has an underlying scoring component [19]-[21]. As a result of the CVSS assessment, the overall severity of IPv6 EHs threat was rated 9.6, in which the severity is categorized as in the critical level and the base score was computed as 8.6 which is assessed as a high level, see Figures 6 and 7. This vulnerability is remotely exploitable and the malicious code can be executed from network hops away or across network layer 3 boundaries from one or more routers as long as the internet is present. In terms of attack complexity, the attacker can expect repeatable attacks against the vulnerable network. Privileges and user interaction are not required to perform this attack. Anyone who has the knowledge, tools, and know the IP address of the target network, the payloads can deliver repeatedly.

However, for the impact metrics, confidentiality and integrity were not greatly affected by this attack but, there is a total loss of availability resulting in the attacker being fully denied access to network resources through DoS attack and affecting not only the target system but all systems connected in the same subnet. Loss of availability presents a direct adverse effect to the affected component, if the attacker cannot deny current connections, it can deny a new one; this attack is repeatable, every instance of a successful attack will lead to leaking of a small amount of memory causing the service to become completely unavailable. The temporal score was computed as 8. 3 which concludes that it is also in the High level, see Figures 6 and 8. The exploit code maturity in this attack worked in every situation. The exploitation tools are widely available on the internet and are easy to use. While the remediation level is very limited and no fix is permanently offered by the vendors. Further, the environmental score was also rated as Critical stage (9.6), see Figures 6 and 9. Moreover, the successful attack is likely to have a catastrophic adverse effect not only on the individual but on the organization environment as a whole. The vector string below was derived based on the inputs from the CVSS which serve as a metric value to determine its scores.

CVSS v3.1 Vector

AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H/E:H/RL:T/RC:C/CR:L/IR:L/AR:H/MAV:N/MAC:L/MPR:N/MUI:N/MS:C/MC:N/MI:N/MA:H

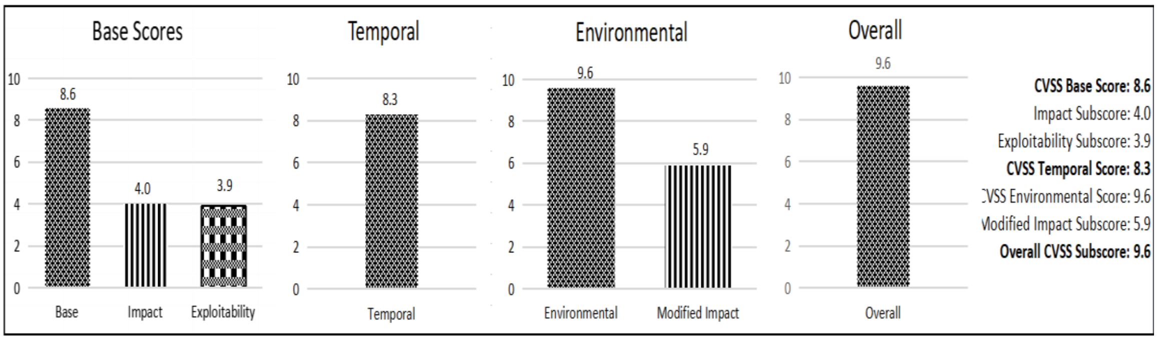
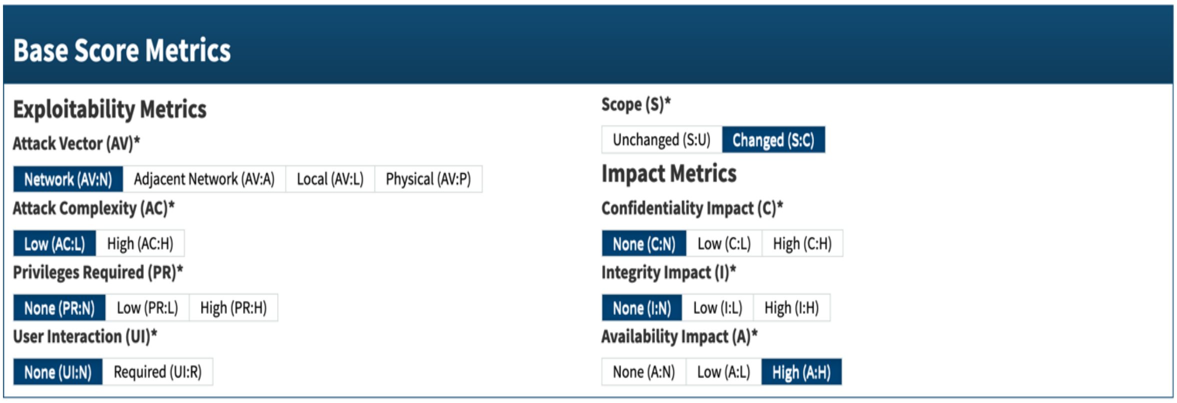


Figure 6. CVSS of IPv6 EHs vulnerabilities



Base Score Metrics

Exploitability Metrics

Attack Vector (AV)*

[✓ Network (AV:N)] Adjacent Network (AV:A) Local (AV:L) Physical (AV:P)

Attack Complexity (AC)*

[✓ Low (AC:L)] High (AC:H)

Privileges Required (PR)*

[✓ None (PR:N)] Low (PR:L) High (PR:H)

User Interaction (UI)*

[✓ None (UI:N)] Required (UI:R)

Scope (S)*

Unchanged (S:U) [✓ Changed (S:C)]

Impact Metrics

Confidentiality Impact (C)*

[✓ None (C:N)] Low (C:L) High (C:H)

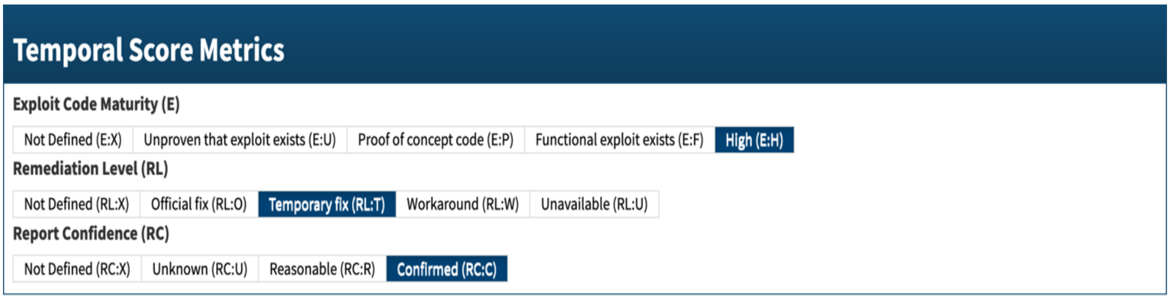
Integrity Impact (I)*

[✓ None (I:N)] Low (I:L) High (I:H)

Availability Impact (A)*

None (A:N) Low (A:L) [✓ High (A:H)]

Figure 7. CVSS of base metrics



Temporal Score Metrics

Exploit Code Maturity (E)

Not Defined (E:X) Unproven that exploit exists (E:U) Proof of concept code (E:P) Functional exploit exists (E:F) [✓ High (E:H)]

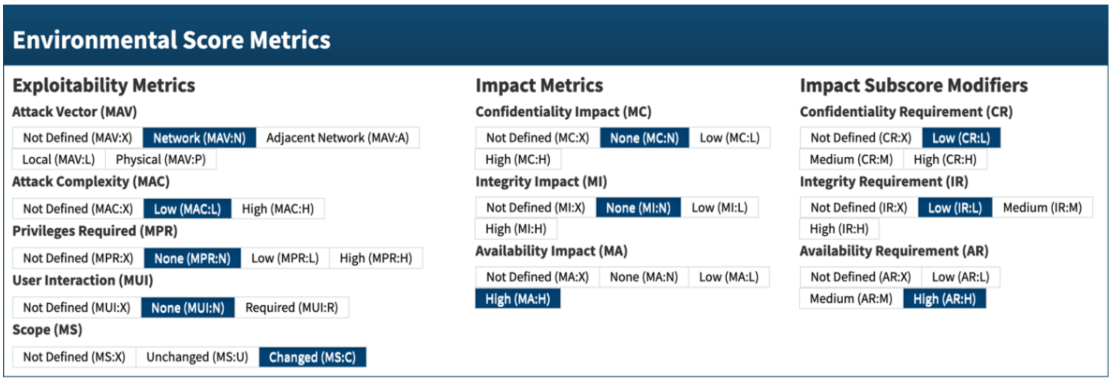
Remediation Level (RL)

Not Defined (RL:X) Official fix (RL:O) [✓ Temporary fix (RL:T)] Workaround (RL:W) Unavailable (RL:U)

Report Confidence (RC)

Not Defined (RC:X) Unknown (RC:U) Reasonable (RC:R) [✓ Confirmed (RC:C)]

Figure 8. CVSS of temporal metrics



Environmental Score Metrics

Exploitability Metrics

Attack Vector (MAV)

Not Defined (MAV:X) [✓ Network (MAV:N)] Adjacent Network (MAV:A) Local (MAV:L) Physical (MAV:P)

Attack Complexity (MAC)

Not Defined (MAC:X) [✓ Low (MAC:L)] High (MAC:H)

Privileges Required (MPR)

Not Defined (MPR:X) [✓ None (MPR:N)] Low (MPR:L) High (MPR:H)

User Interaction (MUI)

Not Defined (MUI:X) [✓ None (MUI:N)] Required (MUI:R)

Scope (MS)

Not Defined (MS:X) Unchanged (MS:U) [✓ Changed (MS:C)]

Impact Metrics

Confidentiality Impact (MC)

Not Defined (MC:X) [✓ None (MC:N)] Low (MC:L) High (MC:H)

Integrity Impact (MI)

Not Defined (MI:X) [✓ None (MI:N)] Low (MI:L) High (MI:H)

Availability Impact (MA)

Not Defined (MA:X) None (MA:N) Low (MA:L) [✓ High (MA:H)]

Impact Subscore Modifiers

Confidentiality Requirement (CR)

Not Defined (CR:X) [✓ Low (CR:L)] Medium (CR:M) High (CR:H)

Integrity Requirement (IR)

Not Defined (IR:X) [✓ Low (IR:L)] Medium (IR:M) High (IR:H)

Availability Requirement (AR)

Not Defined (AR:X) Low (AR:L) Medium (AR:M) [✓ High (AR:H)]

Figure 9. CVSS of environmental metrics

3.3. Mitigation and countermeasures

From the time of writing, the researchers found out that the vendors do not have any permanent remediation on the security issues containing the IPv6 EHs threat. However, some of the traditional approaches seem useful until today. A quick and dirty approach should be considered as one of the effective ways of defending against the threat, but it is also considered as only temporary. The approach can be applied by discarding the inbound/outbound of specific IPv6 EHs using the firewall policy rule [22]-[24]. IETF also advises and recommends this approach, discarding such IPv6 packets can help mitigate the security issues that arise from the use of excessive IPv6 EHs [21]. But, be careful in this approach, because discarding packets containing specific EHs has an operational and interoperability impact on the network operation that would break some of the protocols that rely on it for proper functioning [25].

4. CONCLUSION

The study revealed that up to date, there is no permanent remediation that prevents the IPv6 EHs attack from invading the open-source firewalls by default. By the use of the IPv6 packet manipulations technique, the attacker can easily evade the target network including the target host. Also, CVSS scoring revealed that the base, temporal, and environment metric groups of IPv6 EHs vulnerabilities were in the level of severity. Total loss of network availability presents a direct serious concern in this study. The attack can seriously affect the target component's network connectivity by repeatedly exploiting the vulnerability in each instance of a successful attack, leaking only a small amount of memory, but after repeated successful exploitation causes a network service to become completely unavailable. The successful attack is likely to have a harmful effect not only on the individual but on the organization environment. The network administrator should address these issues seriously by finding the right remedy to counter the threat before the deployment or before the attacker launches the attacks. However, the study has shown that the quick and dirty solution is still one of the effective ways of defending against the EHs packet manipulation attacks, but this is only a temporary one. This study also recommends that the vendors should consider IPv6 EHs packet manipulations as a serious threat, and it should be included in their default/community security ruleset.

ACKNOWLEDGEMENTS

The authors would like to acknowledge and thank the Central Luzon State University and PCARI PRIME Project for allowing us to use their network equipment and to use their network infrastructure for the implementation and testing of our experiments.

REFERENCES

[1] T. Favale, F. Soro, M. Trevisan, I. Drago and M. Mellia, “Campus traffic and e-Learning during COVID-19 pandemic,” *Computer Networks*, vol. 176, no. 107290, 2020, doi: 10.1016/j.comnet.2020.107290.

[2] F. Li and D. Freeman, "Towards A User-Level Understanding of IPv6 Behavior", *Proceedings of the ACM Internet Measurement Conference*, 428–442, 2020, doi:10.1145/3419394.3423618.

[3] APNIC, “2020 APNIC Survey Report,” *Asia Pacific Network Information Centre*, Brisbane, Australia, 2020.

[4] S. Deering and R. Hinden, “Internet Protocol, Version 6 (IPv6) Specification,” *STD 86, RFC 8200*, 2017, doi: 10.17487/RFC8200.

[5] A. Al-Ani, M. Anbar, S. A. Laghari and A. K. Al.-Ani, “Mechanism to prevent the abuse of IPv6 fragmentation in OpenFlow networks,” *PLOS ONE*, vol. 15, no. 5, pp. 1-18, 2020, doi: 10.1371/journal.pone.0232574.

[6] M. A. Naagas, E. L. Mique Jr, T. D. Palaoag and J. S. D. Cruz, “Defense-through-Deception Network Security Model: Securing University Campus Network from DOS/DDOS Attack,” *Bulletin of Electrical Engineering and Informatics*, vol. 7, no. 4, pp. 593-600, 2018, doi: 10.11591/eei.v7i4.1349.

[7] F. Gont, “Security Implications of Predictable Fragment Identification Values,” *RFC 7739*, 2016. doi: 10.17487/RFC7739.

[8] F. Gont, N. Hilliard, G. Doering, W. Kumari, G. Huston and W. Liu, “Operational Implications of IPv6 Packets with Extension Headers,” *RFC 9098*, 2021, doi: 10.17487/RFC9098.

[9] C. Ottow, F. van Vliet, P. de Boer and A. Pras, "The Impact of IPv6 on Penetration Testing", *18th European Conference on Information and Communications Technologies*, pp. 88-99, 2012, doi: 10.1007/978-3-642-32808-4_9.

[10] L. Hendriks, P. Velan, R. d. O. Schmidt, P. de Boer and A. Pras, "Threats and surprises behind IPv6 extension headers," *2017 Network Traffic Measurement and Analysis Conference (TMA)*, 2017, pp. 1-9, doi: 10.23919/TMA.2017.8002912.

[11] M. A. Naagas, A. R. Malicdem and T. D. Palaoag, “DEH-DoSv6: A defendable security model against IPv6 extension headers denial of service attack,” *Bulletin of Electrical Engineering and Informatics*, vol. 10, no. 1, pp. 274-282, 2021, doi: 10.11591/eei.v10i1.2670.

[12] S. Debbarma and P. Debnath, "Internet protocol version 6 (IPv6) Extension Headers: Issues, challenges and mitigation," *2015 2nd International Conference on Computing for Sustainable Global Development (INDIACom)*, 2015, pp. 923-928.

[13] K. Scarfone and P. Hoffman, “Guidelines on Firewalls and Firewall Policy,” *National Institute of Standards and Technology Special Publication*, no. 800-41, pp. 1-48, 2009, doi: 10.6028/NIST.SP.800-41r1.

[14] M. Babik *et al.*, "IPv6 Security," *Journal of Physics: Conference Series*, vol. 898, no. 10, p. 102008, 2017, doi:10.1088/1742-6596/898/10/102008.

[15] M. Käo and J. Žorž, "Requirements for IPv6 in ICT Equipment," RIPE Network Coordination Centre, 2012. [Online]. Available: https://www.ripe.net/publications/docs/ripe-554

[16] A. Khraisat, I. Gondal, P. Vemplew and J. Kamruzzaman, “Survey of intrusion detection systems: techniques, datasets and challenges,” *Cybersecurity*, vol. 2, no. 20, pp. 1-22, 2019, doi: 10.1186/s42400-019-0038-7.

[17] Y. Yin *et al.*, "An Analysis Method for IPv6 Firewall Policy," *2019 IEEE 21st International Conference on High Performance Computing and Communications; IEEE 17th International Conference on Smart City; IEEE 5th International Conference on Data Science and Systems (HPCC/SmartCity/DSS)*, 2019, pp. 1757-1762, doi: 10.1109/HPCC/SmartCity/DSS.2019.00241.

[18] A. Bdair, R. Abdullah, S. Manickam and A. Al-Ani, "Brief of Intrusion Detection Systems in Detecting ICMPv6 Attacks", *Lecture Notes in Electrical Engineering*, pp. 199-213, 2020, doi: 10.1007/978-981-15-0058-9_20.

[19] P. Mell, K. Scarfone and S. Romanosky, “The Common Vulnerability Scoring System (CVSS) and Its Applicability to Federal Agency Systems,” *National Institute of Standards and Technology*, Gaithersburg Rep. no. 7345, 2007.

[20] A. Rosli, A. M. Taib, H. Baharin, W. N. A. W. Ali and R. S. Hamid, “Enhanced Risk Assessment Equation for IPv6 Deployment,” *Proceedings of the 5th International Conference on Computing and Informatics*, pp. 403-409, 2015.

[21] A. Khazaei, M. Ghasemzadeh, and V. Derhami, “An automatic method for CVSS score prediction using vulnerabilities description,” *Journal of Intelligent & Fuzzy Systems*, vol. 30, no. 1, pp. 89-96, 2016, doi: 10.3233/IFS-151733.

[22] M. Verovko, O. Verovko, V. Kazymyr, J. N. Davies and V. Grout, "Performance concerns when implementing infrastructure security in IPv4/IPv6 networks," *2015 Internet Technologies and Applications (ITA)*, pp. 186-191, 2015, doi: 10.1109/ITechA.2015.7317393.

[23] A. Atlasis, “Security Impacts of Abusing IPv6 Extension Headers,” *Black Hat Security Abu Dhabi Conference*, pp. 1–10, 2012.

[24] A. Atlasis, E. Rey, and R. Schaefer, “Evasion of High-End IDPS Devices at the IPv6 Era,” 2017. [Online]. Available: https://www.blackhat.com/docs/eu-14/materials/eu-14-Atlasis-Evasion-Of-High-End-IDPS-Devices-At-The-IPv6-Era-wp.pdf

[25] F. Gont, W. Liu, R. Bonica, “Recommendations on the Filtering of IPv6 Packets Containing IPv6 Extension Headers,” *Internet Engineering Task Force (IETF)*, 2021.

BIOGRAPHIES OF AUTHORS

Anazel P. Gamilla holds a Master’s degree in Information Technology (MIT) from Tarlac State University (TSU), Philippines. An Instructor of the Information Technology Department, College of Engineering, former Chief of Management Information Systems Office at Central Luzon State University (CLSU) and a Department of Information Technology and Communications Technology (DICT-ILCDB) trainer. Her current research interests include computer networks, SDN and cyber security. She can be contacted at email: apgamilla@clsu.edu.ph.

Marlon A. Naagas holds a Doctorate degree in Information Technology (DIT) from the University of the Cordilleras as a CHED Scholar. He is a CHIEF of Management Information System Office (MISO) and also an Assistant Professor IV of Department of Information Technology, College of Engineering at Central Luzon State University. He is a CISCO CyberSecurity Scholarship Awardee, passed CISCO Certified Network Associate in Cyber Security Operations (CCNA-CyberOps) and CISCO Certified CyberOperation Associate. He is associated to DICT-ILCDB as a trainer. Also, he is heavily Involved in collaborative projects of DOST-ASTI, UPEEEI and CLSU such as Bayanihanets, ASI@Connect-Scimix and CHED PCARI-Prime as a network and technical consultant. He can be contacted at email: manaagas@clsu.edu.ph.