Security #7067 CLOSED

defrag: off by one leads to possible evasion

Added by Philippe Antoine almost 2 years ago. Updated over 1 year ago.

Status:	Closed		
Priority:	Normal		
Assignee:	Philippe Antoine		
Target version:	8.0.0-beta1		
Affected Versions:		**Git IDs:**	
Label:		**Severity:**	HIGH
CVE:	2024-45796	**Disclosure Date:**	09/04/2024

Description

Found by oss-fuzz
https://bugs.chromium.org/p/oss-fuzz/issues/detail?id=69475

Regression on 26th of April cf
https://github.com/OISF/suricata/compare/ad4185b3c4fdcdfd0eac44a5ddf6bc7484c35bda...4fedba11404ea6548fd2ed319adf4b78a56180b4

Victor, I leave you this new one, cc @Jason Ish

Files

lolc.pcap (129 KB)	Philippe Antoine, 06/11/2024 08:15 AM	
lole.pcap (300 Bytes)	Philippe Antoine, 06/11/2024 08:55 AM	

Subtasks 1 (0 open — 1 closed)

~~Security #7215~~: defrag: off by one leads to possible evasion (7.0.x backport)	Closed	Philippe Antoine	...

History | Notes | Property changes

PA Updated by Philippe Antoine almost 2 years ago #1

Ouch `tracker->ip_hdr_offset` 4 is greater than `GET_PKT_LEN(r)` 0

VJ Updated by Victor Julien almost 2 years ago #2

Do you have pcap?

PA Updated by Philippe Antoine almost 2 years ago #3

- **File** *lol.pcap* added

The pcap does trigger only on fuzz_decodepcapfile, not on suricata

PA Updated by Philippe Antoine almost 2 years ago #4

- **File** lolc.pcap added

Here is a pcap reproducer

I had to do `mergecap -a -w lolc.pcap lolb.pcap lolb.pcap` because fuzzing runs the input twice (to check for leaks)

PA Updated by Philippe Antoine almost 2 years ago #5

- **File** deleted (~~*lol.pcap*~~)

PA Updated by Philippe Antoine almost 2 years ago #6

- **File** lole.pcap added

Minimized reproducer

VJ Updated by Victor Julien almost 2 years ago #7

- **Status** changed from *New* to *Assigned*

PA Updated by Philippe Antoine almost 2 years ago #8

- **Status** changed from *Assigned* to *In Review*

Gitlab MR

PA Updated by Philippe Antoine over 1 year ago #9

- **Label** *Needs backport to 7.0* added

OT Updated by OISF Ticketbot over 1 year ago #10

- **Subtask** *#7215* added

OT Updated by OISF Ticketbot over 1 year ago #11

- **Label** deleted (~~*Needs backport to 7.0*~~)

PA Updated by Philippe Antoine over 1 year ago #12

- **Tracker** changed from *Bug* to *Security*
- **Severity** set to *MODERATE*
- **Disclosure Date** set to *09/04/2024*

VJ Updated by Victor Julien over 1 year ago #13

- **Assignee** changed from *Victor Julien* to *Philippe Antoine*

VJ Updated by Victor Julien over 1 year ago #14

- **Severity** changed from *MODERATE* to *HIGH*

HIGH as it could potentially lead to loss of visibility, and thus policy bypass.

VJ Updated by Victor Julien over 1 year ago #15

- **Subject** changed from *defrag: DEBUG_VALIDATE_BUG_ON(len > UINT16_MAX);* to *defrag: off by one leads to possible evasion*

JF Updated by Juliana Fajardini Reichow over 1 year ago #16

- **CVE** set to *2024-45796*

https://github.com/OISF/suricata/security/advisories/GHSA-mf6r-3xp2-v7xg

PA Updated by Philippe Antoine over 1 year ago #17

- **Status** changed from *In Review* to *Closed*

https://github.com/OISF/suricata/commit/9203656496c4081260817cce018a0d8fd57869b5

VJ Updated by Victor Julien over 1 year ago #18

- **Private** changed from *Yes* to *No*