Security #7195 CLOSED

datasets: rule with unset makes suricata abort

Added by Philippe Antoine over 1 year ago. Updated over 1 year ago.

Status:	Closed		
Priority:	Normal		
Assignee:	Philippe Antoine		
Target version:	8.0.0-beta1		
Affected Versions:		**Git IDs:**	e47598110a557bb9f87ea498d85ba91a45bb0cb6
Label:			
CVE:	2024-45795	**Severity:**	HIGH
		Disclosure Date:	

Description

Running SV datasets-03-set test with added rule

```
diff --git a/tests/datasets-03-set/test.rules b/tests/datasets-03-set/test.rules
index 1d99df9d..327c774a 100644
--- a/tests/datasets-03-set/test.rules
+++ b/tests/datasets-03-set/test.rules
@@ -1 +1,2 @@
 alert dns any any -> any any (dns.query; dataset:set,dns-seen, type string; sid:1;)
+alert dns any any -> any any (dns.query; content: "example"; dataset:unset,dns-seen, type string; s
```

triggers the abort in `DetectDatasetBufferMatch` because we get `DETECT_DATASET_CMD_UNSET`

Subtasks 1 (0 open — 1 closed)

~~Security #7196~~: datasets: rule with unset makes suricata abort (7.0.x backport)	Closed	Philippe Antoine

Related issues 1 (1 open — 0 closed)

Related to Suricata - Feature #5576: Dataset is setting data despite the signature being a complete match	In Review	Philippe Antoine

History | Notes | Property changes

PA Updated by Philippe Antoine over 1 year ago #1

- **Related to** *Feature #5576: Dataset is setting data despite the signature being a complete match* added

OT Updated by OISF Ticketbot over 1 year ago #2

- **Subtask** *#7196* added

OT Updated by OISF Ticketbot over 1 year ago #3

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

PA Updated by Philippe Antoine over 1 year ago #4

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

Gitlab MR

PA Updated by Philippe Antoine over 1 year ago #5

unset support in datasets was half-done.

A fix can be implementing the missing support

Another fix can be to reject such rules for now

VJ Updated by Victor Julien over 1 year ago #6

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

HIGH as it requires a bad rule, but then it aborts in defined way.

JF Updated by Juliana Fajardini Reichow over 1 year ago #7

- **CVE** set to *2024-45795*

https://github.com/OISF/suricata/security/advisories/GHSA-6r8w-fpw6-cp9g

PA Updated by Philippe Antoine over 1 year ago #8

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

https://github.com/OISF/suricata/pull/11815

PA Updated by Philippe Antoine over 1 year ago #9

Still SV test to merge before closing https://github.com/OISF/suricata-verify/pull/2065

PA Updated by Philippe Antoine over 1 year ago #10

- **Git IDs** updated (diff)

VJ Updated by Victor Julien over 1 year ago #11

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

PA Updated by Philippe Antoine over 1 year ago #12

- **Status** changed from *Resolved* to *Closed*

https://github.com/OISF/suricata-verify/pull/2071