integer overflow in whoopsie 0.2.69

Bug #1872560 reported by Seong-Joong Kim on 2020-04-13

This bug affects 1 person

268

Affects	Status	Importance	Assigned to	Milestone
whoopsie (Ubuntu)	Fix Released	High	Marc Deslauriers	
Xenial	Fix Released	High	Marc Deslauriers	
Bionic	Fix Released	High	Marc Deslauriers	
Eoan	Won't Fix	High	Marc Deslauriers	
Focal	Fix Released	High	Marc Deslauriers	
Groovy	Fix Released	High	Marc Deslauriers	

Bug Description

```
Hi,

I have found a security issue on whoopsie 0.2.69 and earlier.

## Vulnerability in whoopsie
- whoopsie 0.2.69 and earlier have a heap-based buffer overflow
vulnerability.
- An attacker can cause a denial of service (memory corruption and
application crash) via a crafted .crash file.

## Basic
When a program has been crashed, Linux system tries to create a '.crash'
file on '/var/crash/' directory with python script located in '/usr/share/
apport/apport'.
The file contains a series of system crash information including core
dump, syslog, stack trace, memory map info, etc.
After the creation of '.crash' file, whoopsie extracts the above
information from the '.crash' file and encodes it into binary json (bson)
format.
Lastly, whoopsie forwards the data to a remotely connected Ubuntu Error
Report system.

## Vulnerability
Unfortunately, we have found a heap-based buffer overflow vulnerability
during the encoding, when whoopsie attempts to bsonify with crafted crash
file.
The data in '.crash' file is stored in key-value form and the whoopsie
separately measures the length of 'key' and 'value' to allocate memory
region during the encoding.
A heap-based buffer overflow can occur when an integer overflow happens on
a variable that contains length of 'key'.
FYI, a issue to that raised by 'value' is well covered by performing
exception handling.

@[bson.c:663][https://git.launchpad.net/ubuntu/+source/whoopsie/tree/lib/
bson/bson.c?h=applied/0.2.69#n663]

const uint32_t len = strlen( name ) + 1;

- Integer overflow occurs when length of ‘name’ exceeds INT32_MAX value.
- Here, ‘name’ indicates the ‘key’ data in ‘.crash’ file.

@[bson.c:627][https://git.launchpad.net/ubuntu/+source/whoopsie/tree/lib/
bson/bson.c?h=applied/0.2.69#n627]

b->data = bson_realloc( b->data, new_size );

- Unexpected small memory region is allocated due to above integer
overflow.

@[bson.c:680][https://git.launchpad.net/ubuntu/+source/whoopsie/tree/lib/
bson/bson.c?h=applied/0.2.69#n680]

bson_append( b, name, len );

- Memory corruption happens when unexpected small memory region is
allocated.

## Attack Scenario
1) Create a fake.crash file
- '.crash' file is composed of the following format: 'key : value'.
- To cause the overflow attack, the size of 'key' should be in double
amount of INT32_MAX.
- The size of 'value' doesn’t matter, but not zero length.

$ python -c "print('A' * 0xFFFFFFFF + ' : ' + 'B')" > /var/crash/
fake.crash
$ cat fake.crash
AAA … AA : B

2) Trigger the whoopsie to read the fake.crash file
- Just create 'fake.upload' file by touch command.
- Or launch apport-gtk gui or apport-bug cli application.

3) Check out the result
- After a while, the whoopsie has been killed by segmentation fault.

Sincerely,
```

Tags: patch

Related branches

lp:whoopsie

CVE References

Report a bug

This report contains **Public Security** information

Everyone can see this security related information.

Duplicates of this bug

You are not directly subscribed to this bug's notifications.

Edit bug mail

Other bug subscribers

Subscribe someone else

Notified of all changes

- Marc Deslauriers
- Seong-Joong Kim
- Ubuntu Review Team
- Ubuntu Security Team

May be notified

- Alejandro J. Alva...
- Ashani Holland
- Bjoern
- Brian Murray
- Bruno Garcia
- CRC
- Calub Viem
- Cemirtan Igor Gri...
- Charlie_Smotherman
- Christina A Reitb...
- David
- Debian PTS
- Dmitriev Artem An...
- Doraann2
- Felix K.
- Franko Fang
- HaySayCheese
- Hidagawa
- Jader Gabriel
- Jesse Jones
- José Alfonso
- Kshitij Mehrotra
- Masoud shokohi
- Matt j
- Matvej Jurbin
- Mr. MInhaj
- Name Changed
- Nick
- PCTeacher012
- Paolo Topa
- Peter Bullert
- Punnsa
- Richard Barnes
- Richard Seguin
- Richard Williams
- Rob Linc
- Rudra Saraswat
- Ryan Garrett
- Simon Quigley
- Tom Weiss
- Ubuntu Foundation...
- Ubuntu Lumina
- Ubuntu Touch seed...
- Vasanth
- Vic Parker
- Warren White
- ahepas
- basilisgabri
- cornelis stravers
- dsfkj dfjx
- dvergspett
- eoininmoran
- ganesh
- ginoballerino
- linuxgijs
- majid hussain
- mmmen
- nikonikic42
- projevie@hotmail.com
- qadir

2020-11937

2020-12135

2020-15570

Seong-Joong Kim (sungjungk) on 2020-04-15

summary:- heap-based buffer overflow on bson.c
+ heap-based buffer overflow in bson.c

Seong-Joong Kim (sungjungk) wrote on 2020-04-16: **Re: heap-based buffer overflow in bson.c** #1

bson-fix-overflow.patch (1.3 KiB, text/plain)

It seems that this vulnerability was originally caused by ‘bytesNeeded’ integer overflow in bson_ensure_space().
Sum of ‘len’ and ‘dataSize’ that both have a type of ‘uint32_t’ can assigned to ‘byteNeeded’ (see https://git.launchpad.net/ubuntu/+source/whoopsie/tree/lib/bson/bson.c?h=applied/0.2.69#n670).
Even though it was already applied a series of exception handling routine for overflow of 'len' and 'dataSize', the flaw lies in improper exception handling of overflow in 'bytesNeeded'.
I think it would be better to replace data type of 'bytesNeeded'; from 'uint32_t' to 'size_t'.
Please check the attached patch.

Seong-Joong Kim (sungjungk) wrote on 2020-04-19: #2

bson-overflow-fixed.patch (460 bytes, text/plain)

I also suggest a solution to deal with it in a different way.

Motivation
A heap-based buffer overflow can occur when an integer overflow happens on a ‘bytesNeeded’ variable.
The followings are required to cause overflow on ‘bytesNeeded’.
- length of ‘value’ in .crash file => 0 < {length of ‘value’} < 1024
- length of ‘key’ in .crash file => UINT32_MAX - {length of ‘value’} - 7 < {length of ‘key’}

To deal with it, it is required the following exception handling after line 663 in bson.c

```
if (len > UINT32_MAX - dataSize - 1)
  return BSON_ERROR;
```

Unfortunately, ‘len’ variable can also occur an integer overflow and it leads to unintended consequences.

To correct the above issues, the following exception handling will be better than the above one.

```
if (len > INT32_MAX)
  return BSON_ERROR;
```

It is reasonable to assume that the length of 'key' in .crash will not exceed INT32_MAX.

Modification
Correct the above issue.
Correctly added exception handling against overflow.

Seong-Joong Kim (sungjungk) on 2020-04-22

information type: Private Security → Public Security

Seong-Joong Kim (sungjungk) wrote on 2020-04-22: #3

I would like to update the contents of 'Attack Scenario'.

from:

```
$ python -c "print('A' * 0xFFFFFFFF + ' : ' + 'B')" > /var/crash/
fake.crash
```

to:

```
$ python -c "print('A' * 0xFFFFFFFE + ' : ' + 'B')" > /var/crash/
fake.crash
```

Segfault can arise when the following requirements are met, as I mentioned above.
- length of ‘value’ in .crash file => 0 < {length of ‘value’} < 1024
- length of ‘key’ in .crash file => UINT32_MAX - {length of ‘value’} - 7 < {length of ‘key’} < UINT32_MAX

Please check this issue.

Ubuntu Foundations Team Bug Bot (crichton) wrote on 2020-04-22: #4

The attachment "bson-fix-overflow.patch" seems to be a patch. If it isn't, please remove the "patch" flag from the attachment, remove the "patch" tag, and if you are a member of the ~ubuntu-reviewers, unsubscribe the team.

[This is an automated message performed by a Launchpad user owned by ~brian-murray, for any issues please contact him.]

tags:added: patch

Seong-Joong Kim (sungjungk) on 2020-04-23

summary:- heap-based buffer overflow in bson.c
+ integer overflow in whoopsie 0.2.69

Sebastien Bacher (seb128) on 2020-04-23

Changed in whoopsie (Ubuntu):
importance: Undecided → High

sankaran

ubuntu18

van

नेपाली भाषा समायो...

Patches

bson-fix-overflow.patch

bson-overflow-fixed.patch

Add patch

tags:added: rls-ff-incoming

Marc Deslauriers (mdeslaur) wrote on 2020-04-23: #5

Hi,

Thanks for reporting this issue. We are currently investigating it.

Marc Deslauriers (mdeslaur) wrote on 2020-04-23: #6

It looks like bson.c in whoopsie was originally taken from here:

https://github.com/10gen-archive/mongo-c-driver-legacy/tree/master/src

The upstream repo has seen a lot of security fixes since the code was
copied, perhaps we should investigate re-syncing it before attempting to
fix it ourselves.

Seth Arnold (seth-arnold) wrote on 2020-04-24: #7

Use CVE-2020-12135.

Thanks

Sebastien Bacher (seb128) on 2020-04-24

Changed in whoopsie (Ubuntu):
status:New → Confirmed

Marc Deslauriers (mdeslaur) wrote on 2020-05-05: #8

Hi,

What release did you use to reproduce this? I tried reproducing it in
Ubuntu 18.04 LTS, but whoopsie parses the file without segfaulting.

I tried both

```
$ python -c "print('A' * 0xFFFFFFFF + ' : ' + 'B')" > /var/crash/
fake.crash
```

and

```
$ python -c "print('A' * 0xFFFFFFFE + ' : ' + 'B')" > /var/crash/
fake.crash
```

Could you give a bit more details on how to reproduce this? Thanks!

Seong-Joong Kim (sungjungk) wrote on 2020-05-06: #9

Thank you for your reply.

Please check the following video.
https://youtu.be/pGfOzcgd5CU

It also affects on whoopsie 0.2.69.

Thanks.

Marc Deslauriers (mdeslaur) wrote on 2020-05-06: #10

Thanks for the video, but I still can't reproduce the issue.

What version of Ubuntu are you running in the video?
How much ram do you have in that machine?
Are you able to reproduce the issue with the pre-compiled version of
Ubuntu that comes with it?

Marc Deslauriers (mdeslaur) wrote on 2020-05-06: #11

Sorry, I meant "Are you able to reproduce the issue with the pre-compiled
version of Whoopsie that comes with it?"

Seong-Joong Kim (sungjungk) wrote on 2020-05-07: #12

Sure. This issue is also reproducible with pre-compiled version of
0.2.62ubuntu0.4.

Marc Deslauriers (mdeslaur) wrote on 2020-06-17: #13

I still can't reproduce this issue.

Seong-Joong Kim (sungjungk) wrote on 2020-06-18: #14

I am utilizing the 8GB of RAM and pre-compiled version of Ubuntu 18.04.

Could you tell me how much ram do you have in that machine?

Brian Murray (brian-murray) on 2020-06-25

Changed in whoopsie (Ubuntu):
status:Confirmed → Incomplete

Marc Deslauriers (mdeslaur) on 2020-07-09

Changed in whoopsie (Ubuntu):
assignee:nobody → Marc Deslauriers (mdeslaur)
status:Incomplete → Confirmed

Marc Deslauriers (mdeslaur) wrote on 2020-07-09: #15 https://github.com/sungjungk/apport-vuln

Marc Deslauriers (mdeslaur) on 2020-07-09

```
Changed in whoopsie (Ubuntu Xenial):
    status:New → Confirmed
Changed in whoopsie (Ubuntu Bionic):
    status:New → Confirmed
Changed in whoopsie (Ubuntu Eoan):
    status:New → Confirmed
Changed in whoopsie (Ubuntu Focal):
    status:New → Confirmed
Changed in whoopsie (Ubuntu Xenial):
importance:Undecided → High
Changed in whoopsie (Ubuntu Bionic):
importance:Undecided → High
Changed in whoopsie (Ubuntu Eoan):
importance:Undecided → High
Changed in whoopsie (Ubuntu Focal):
importance:Undecided → High
Changed in whoopsie (Ubuntu Xenial):
  assignee:nobody → Marc Deslauriers (mdeslaur)
Changed in whoopsie (Ubuntu Bionic):
  assignee:nobody → Marc Deslauriers (mdeslaur)
Changed in whoopsie (Ubuntu Eoan):
  assignee:nobody → Marc Deslauriers (mdeslaur)
Changed in whoopsie (Ubuntu Focal):
  assignee:nobody → Marc Deslauriers (mdeslaur)
```

Launchpad Janitor (janitor) wrote on 2020-08-04: #16

```
This bug was fixed in the package whoopsie - 0.2.69ubuntu0.1

---------------
whoopsie (0.2.69ubuntu0.1) focal-security; urgency=medium

  * SECURITY UPDATE: integer overflow in bson parsing (LP: #1872560)
    - lib/bson/*: updated to latest upstream release.
    - CVE-2020-12135
  * SECURITY UPDATE: resource exhaustion via memory leak (LP: #1881982)
    - src/whoopsie.c, src/tests/test_parse_report.c: properly handle
      GHashTable.
    - CVE-2020-11937
  * SECURITY UPDATE: DoS via large data length (LP: #1882180)
    - src/whoopsie.c, src/whoopsie.h, src/tests/test_parse_report.c: limit
      the size of a report file.
    - CVE-2020-15570

 -- Marc Deslauriers <email address hidden> Fri, 24 Jul 2020 08:55:26
-0400

Changed in whoopsie (Ubuntu Focal):
 status:Confirmed → Fix Released
```

Launchpad Janitor (janitor) wrote on 2020-08-04: #17

```
This bug was fixed in the package whoopsie - 0.2.52.5ubuntu0.5

---------------
whoopsie (0.2.52.5ubuntu0.5) xenial-security; urgency=medium

  * SECURITY UPDATE: integer overflow in bson parsing (LP: #1872560)
    - lib/bson/*: updated to latest upstream release.
    - CVE-2020-12135
  * SECURITY UPDATE: resource exhaustion via memory leak (LP: #1881982)
    - src/whoopsie.c, src/tests/test_parse_report.c: properly handle
      GHashTable.
    - CVE-2020-11937
  * SECURITY UPDATE: DoS via large data length (LP: #1882180)
    - src/whoopsie.c, src/whoopsie.h, src/tests/test_parse_report.c: limit
      the size of a report file.
    - CVE-2020-15570

 -- Marc Deslauriers <email address hidden> Fri, 24 Jul 2020 08:55:26
-0400

Changed in whoopsie (Ubuntu Xenial):
 status:Confirmed → Fix Released
```

Launchpad Janitor (janitor) wrote on 2020-08-04: #18

```
This bug was fixed in the package whoopsie - 0.2.62ubuntu0.5

---------------
whoopsie (0.2.62ubuntu0.5) bionic-security; urgency=medium

  * SECURITY UPDATE: integer overflow in bson parsing (LP: #1872560)
    - lib/bson/*: updated to latest upstream release.
    - CVE-2020-12135
  * SECURITY UPDATE: resource exhaustion via memory leak (LP: #1881982)
    - src/whoopsie.c, src/tests/test_parse_report.c: properly handle
      GHashTable.
    - CVE-2020-11937
  * SECURITY UPDATE: DoS via large data length (LP: #1882180)
    - src/whoopsie.c, src/whoopsie.h, src/tests/test_parse_report.c: limit
      the size of a report file.
    - CVE-2020-15570

 -- Marc Deslauriers <email address hidden> Fri, 24 Jul 2020 08:55:26
-0400

Changed in whoopsie (Ubuntu Bionic):
 status:Confirmed → Fix Released
```

Brian Murray (brian-murray) on 2020-08-06

```
  tags:removed: rls-ff-incoming
Changed in whoopsie (Ubuntu Eoan):
 status:Confirmed → Won't Fix
Changed in whoopsie (Ubuntu Groovy):
 status:Confirmed → Fix Committed
```

Launchpad Janitor (janitor) wrote on 2020-08-07: #19

```
This bug was fixed in the package whoopsie - 0.2.71

---------------
whoopsie (0.2.71) groovy; urgency=medium

  [ Marc Deslauriers ]
  * SECURITY UPDATE: integer overflow in bson parsing (LP: #1872560)
    - lib/bson/*: updated to latest upstream release.
    - CVE-2020-12135
  * SECURITY UPDATE: resource exhaustion via memory leak (LP: #1881982)
    - src/whoopsie.c, src/tests/test_parse_report.c: properly handle
      GHashTable.
    - CVE-2020-11937
  * SECURITY UPDATE: DoS via large data length (LP: #1882180)
    - src/whoopsie.c, src/whoopsie.h, src/tests/test_parse_report.c: limit
      the size of a report file.
    - CVE-2020-15570

 -- Brian Murray <email address hidden> Wed, 05 Aug 2020 15:00:45 -0700

Changed in whoopsie (Ubuntu Groovy):
status:Fix Committed → Fix Released
```

See full activity log

To post a comment you must log in.

Launchpad • Take the tour • Read the guide