DoS vulnerability: cause resource exhaustion

Bug #1881982 reported by Seong-Joong Kim on 2020-06-04

This bug affects 1 person

262

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

Bug Description

Hi,

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

# Vulnerability description
The parse_report() function in whoopsie.c allows attackers to cause a denial of service (memory leak) via a crafted file.
Exploitation of this issue causes excessive memory consumption which results in the Linux kernel triggering OOM killer on arbitrary process.
This results in the process being terminated by the OOM killer.

# Details
We have found a memory leak vulnerability during the parsing the crash file, when a collision occurs on GHashTable through g_hash_table_insert().
According to [1], if the key already exists in the GHashTable, its current value is replaced with the new value.
If 'key_destory_func' and 'value_destroy_func' are supplied when creating the table, the old value and the passed key are freed using that function.
Unfortunately, whoopsie does not handle the old value and the passed key when collision happens.
If a crash file contains same repetitive key-value pairs, it leads to memory leak as much as the amount of repetition and results in denial-of-service.

[1] https://developer.gnome.org/glib/stable/glib-Hash-Tables.html#g-hash-table-insert

# PoC (*Please check the below PoC: whoopsie_killer.py)
1) Generates a certain malformed crash file that contains same repetitive key-value pairs.
2) Trigger the whoopsie to read the generated crash file.
3) After then, the whoopsie process has been killed.

# Mitigation (*Please check the below patch: g_hash_table_memory_leak.patch)
We should use g_hash_table_new_full() with ‘key_destroy_func’ and ‘value_destroy_func’ functions instead of g_hash_table_new().
Otherwise, before g_hash_table_insert(), we should check the collision via g_hash_table_lookup_extended() and obtain pointer to the old value and remove it.

Sincerely,

See original description

Tags: patch

Related branches

lp:whoopsie

CVE References

2020-11937

2020-12135

2020-15570

Seong-Joong Kim (sungjungk) wrote on 2020-06-10: #2

g_hash_table_memory_leak.patch (1.9 KiB, text/plain)

Modification:
Correct the above issue.
Replace g_hash_table_new() with g_hash_table_new_full() and add 'key_destroy_func' and 'value_destroy_func' function.

Seong-Joong Kim (sungjungk) on 2020-06-10

description: updated

Seong-Joong Kim (sungjungk) on 2020-06-11

information type: Private Security → Public Security

Ubuntu Foundations Team Bug Bot (crichton) wrote on 2020-06-11: #3

The attachment "g_hash_table_memory_leak.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.

Report a bug

This report contains **Public Security** information

Everyone can see this security related information.

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

Edit bug mail

Other bug subscribers

Subscribe someone else

Notified of all changes

- Kai Kasurinen
- Seong-Joong Kim
- Ubuntu Review Team
- Ubuntu Sponsors 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
- Marc Deslauriers
- 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 Security Team
- 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

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

```
tags:added: patch
```

Mathew Hodson (mhodson) on 2020-06-13

```
Changed in whoopsie (Ubuntu):
importance:Undecided → Medium
```

Seong-Joong Kim (sungjungk) wrote on 2020-06-15: #4

This vulnerability may cause a memory exhaustion vulnerability in the
function parse_report() in whoopsie.c, which allows attackers to cause a
denial of service.

Seong-Joong Kim (sungjungk) on 2020-06-16

```
summary:- Memory leak in parse_report()
        + memory exhaustion in parse_report()
```

Seong-Joong Kim (sungjungk) on 2020-06-16

```
description:updated
```

Seong-Joong Kim (sungjungk) wrote on 2020-06-18: **Re: memory exhaustion in parse_report()** #5

whoopsie_killer.py (3.1 KiB, text/x-python)

Exploitation of this issue causes excessive memory consumption which
results in the Linux kernel triggering OOM killer on arbitrary process.
This results in the process being terminated by the OOM killer.
Please check the following PoC: whoopsie_killer.py

Seong-Joong Kim (sungjungk) on 2020-06-19

```
description:updated
    summary:- memory exhaustion in parse_report()
            + DoS vulnerability: cause resource exhaustion
```

Leonidas S. Barbosa (leosilvab) on 2020-07-06

```
Changed in whoopsie (Ubuntu):
  status:New → Confirmed
assignee:nobody → Alex Murray (alexmurray)
```

Marc Deslauriers (mdeslaur) on 2020-07-09

```
Changed in whoopsie (Ubuntu):
assignee:Alex Murray (alexmurray) → Marc Deslauriers (mdeslaur)
```

Marc Deslauriers (mdeslaur) wrote on 2020-07-09: #6

https://github.com/sungjungk/whoopsie_killer

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 → Medium
Changed in whoopsie (Ubuntu Bionic):
importance:Undecided → Medium
Changed in whoopsie (Ubuntu Eoan):
importance:Undecided → Medium
Changed in whoopsie (Ubuntu Focal):
importance:Undecided → Medium
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)
```

Seth Arnold (seth-arnold) wrote on 2020-07-09: #7

Please use CVE-2020-11937 for this issue. Thanks.

Launchpad Janitor (janitor) wrote on 2020-08-04: #8

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
```

sankaran
ubuntu18
van
नेपाली भाषा समायो...

Patches

g_hash_table_memory_leak.patch

Add patch

Bug attachments

whoopsie_killer.py

Add attachment

```
  * 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: #9

```
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: #10

```
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

Launchpad Janitor (janitor) wrote on 2020-08-07: #11

```
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:Confirmed → Fix Released

Brian Murray (brian-murray) wrote on 2020-08-18: #12

```
The Eoan Ermine has reached end of life, so this bug will not be fixed for
that release
```

Changed in whoopsie (Ubuntu Eoan):
status:Confirmed → Won't Fix

See full activity log

To post a comment you must log in.