

Bug 1975489 (CVE-2021-3622) - CVE-2021-3622 hivex: stack overflow due to recursive call of _get_children()

Keywords:

Security ×

Status: CLOSED ERRATA

Alias: CVE-2021-3622

Product: Security Response

Component: vulnerability 🛠️

Version: unspecified

Hardware: All

OS: Linux

Priority: low

Severity: low

Target ---

Milestone ---

Assignee: Red Hat Product Security

QA Contact:

Docs Contact:

URL:

Whiteboard:

Depends On: 🚩 1976193 🚩 1976194 🚩 1976195 🚩 1976196 🚩 4080400

Blocks: 🚩 1975490 🚩 1976188

TreeView+ depends on / blocked

Reported: 2021-06-23 19:19 UTC by Pedro Sampaio

Modified: 2022-05-10 13:16 UTC (History)

CC List: 7 users (show)

Fixed In Version: hivex-1.3.21

Doc Type: ⓘ If docs needed, set a value

Doc Text: ⓘ A flaw was found in the hivex library. This flaw allows an attacker to input a specially crafted Windows Registry (hive) file, which would cause hivex to recursively call the _get_children() function, leading to a stack overflow. The highest threat from this vulnerability is to system availability.

Clone Of:

Environment:

Last Closed: 2021-08-31 18:56:15 UTC

Attachments		(Terms of Use)
hivex_crash.zip (693 bytes, application/zip) 2021-07-08 17:41 UTC, Richard W.M. Jones	no flags	Details
0001-lib-node.c-limit-recursion-in-ri-records-CVE-2021-36.patch (3.21 KB, patch) 2021-07-08 18:08 UTC, Richard W.M. Jones	no flags	Details Diff
Add an attachment (proposed patch, testcase, etc.)		View All

Links						
System	ID	Private	Priority	Status	Summary	Last Updated
Red Hat Product Errata	RHSA-2021:3338	0	None	None	None	2021-08-31 09:11:49 UTC
Red Hat Product Errata	RHSA-2022:1759	0	None	None	None	2022-05-10 13:16:40 UTC

Pedro Sampaio 2021-06-23 19:19:37 UTC

Description

A flaw was found in libhivex. A stack overflow occurs as the children of each listed node grows. This causes the _get_children function to continue calling until it eventually overflows the stack and causes the program to crash.

References:

<https://github.com/libguestfs/hivex/commit/771728218dac2fbf6997a7e53225e75a4c6b7255>
<https://listman.redhat.com/archives/libguestfs/2021-August/msg00002.html>

Richard W.M. Jones 2021-07-08 17:41:40 UTC

Comment 5

Created attachment 1799722 [details]
hivex_crash.zip

Reproducer hive is attached. (Note it's a password encrypted ZIP file, the password is "hivex".)

Richard W.M. Jones 2021-07-08 17:46:15 UTC

Comment 6

I can only reproduce this bug using ASAN. Here's how:

(1) Clone hivex from git (<https://github.com/libguestfs/hivex>)

(2) Compile with:

```
./autogen.sh \
CFLAGS="-fsanitize=address,undefined -fno-omit-frame-pointer -g -O2 -fPIC"
```

make

(3) Run the following command to start the hivex shell:

```
./sh/hivexsh -u id\000008\,sig\11\,src\000325+000218\,time\386722627\,op\splice\,rep\16
```

(4) Type "ls" at the shell prompt.

```
id\000008,sig\11,src\000325+000218,time\386722627,op\splice,rep\16> ls
AddressSanitizer:DEADLYSIGNAL
=====
==1365280==ERROR: AddressSanitizer: stack-overflow on address 0x7fffd82f1ff8 (pc 0x7f4ae2736c18 bp 0x7fffd82f2010 sp 0x7fffd82f2000 T0)
#0 0x7f4ae2736c18 in _hivex_add_to_offset_list /home/rjones/d/hivex/lib/offset-list.c:69
#1 0x7f4ae273132a in _get_children /home/rjones/d/hivex/lib/node.c:389
#2 0x7f4ae2731726 in _get_children /home/rjones/d/hivex/lib/node.c:489
#3 0x7f4ae2731726 in _get_children /home/rjones/d/hivex/lib/node.c:489
#4 0x7f4ae2731726 in _get_children /home/rjones/d/hivex/lib/node.c:489
...
#247 0x7f4ae2731726 in _get_children /home/rjones/d/hivex/lib/node.c:489
#248 0x7f4ae2731726 in _get_children /home/rjones/d/hivex/lib/node.c:489
SUMMARY: AddressSanitizer: stack-overflow /home/rjones/d/hivex/lib/offset-list.c:69 in _hivex_add_to_offset_list
==1365280==ABORTING
```

Richard W.M. Jones 2021-07-08 17:51:27 UTC

Comment 7

So even without ASAN, the code recursively calls `_get_children` and it would cause a stack overflow. Probably ASAN makes the stack frames a bit larger causing the error to happen with a smaller hive.

It appears to be a security issue similar in severity to the last one that was reported ([bug-1343667](#)).

Richard W.M. Jones 2021-07-08 18:08:44 UTC

[Comment 8](#)

Created [attachment 1799738](#) [details]

0001-lib-node.c-Limit-recursion-in-ri-records-CVE-2021-36.patch

With this patch you will see an error like this instead of a crash:

```
\> ls
hivex: _get children: returning EINVAL because: ri-record nested to depth >= 32
ls: Invalid argument
```

Richard W.M. Jones 2021-07-08 20:22:40 UTC

[Comment 9](#)

FWIW I ran an instrumented version of hivex over a small collection of real registry hives that I keep, and none of them had depth > 1. So in my opinion this patch is unlikely to affect any real hives that we would encounter.

Mauro Matteo Cascella 2021-07-09 08:50:36 UTC

[Comment 11](#)

In reply to [comment #7](#):

```
> So even without ASAN, the code recursively calls _get_children
> and it would cause a stack overflow. Probably ASAN makes the
> stack frames a bit larger causing the error to happen with a
> smaller hive.
>
> It appears to be a security issue similar in severity to the last
> one that was reported (bug-1343667).
```

Thanks for your comments and testing, Richard. I'd keep this flaw low severity, as it doesn't seem to have any direct impact on confidentiality/integrity, and only partial unavailability for the same reasons as the last one (i.e., the user can always retry the operation && a crash in hivex would not result in a crash in libguestfs).

Richard W.M. Jones 2021-08-02 08:09:42 UTC

[Comment 17](#)

Since the embargo date has passed, this bug has now been made public:

<https://github.com/libguestfs/hivex/commit/771728218dac2fbf6997a7e53225e75a4c6b7255>
<https://listman.redhat.com/archives/libguestfs/2021-August/msg00002.html>

Mauro Matteo Cascella 2021-08-02 15:54:44 UTC

[Comment 18](#)

Created hivex tracking bugs for this issue:

Affects: fedora-all [[bug-1369150](#)]

errata-xmlrpc 2021-08-31 09:11:47 UTC

[Comment 20](#)

This issue has been addressed in the following products:

Red Hat Enterprise Linux 7
Via RHSA-2021:3338 <https://access.redhat.com/errata/RHSA-2021:3338>

Product Security DevOps Team 2021-08-31 18:56:15 UTC

[Comment 21](#)

This bug is now closed. Further updates for individual products will be reflected on the CVE page(s):

<https://access.redhat.com/security/cve/cve-2021-3622>

errata-xmlrpc 2022-05-10 13:16:38 UTC

[Comment 22](#)

This issue has been addressed in the following products:

Red Hat Enterprise Linux 8
Via RHSA-2022:1759 <https://access.redhat.com/errata/RHSA-2022:1759>

Note
You need to [log in](#) before you can comment on or make changes to this bug.