**linuxppc-dev.lists.ozlabs.org archive mirror**

search help / color / mirror / Atom feed

```
* Linux kernel: powerpc: KVM guest to host memory corruption
@ 2021-07-26  9:13 Michael Ellerman
  2021-07-27  0:46 ` Michael Ellerman
  0 siblings, 1 reply; 2+ messages in thread
From: Michael Ellerman @ 2021-07-26  9:13 UTC (permalink / raw)
  To: oss-security; +Cc: linuxppc-dev
```

The Linux kernel for powerpc since v3.10 has a bug which allows a malicious KVM guest to corrupt host memory.

In the handling of the H_RTAS hypercall, args.rets is made to point into the args.args buffer which is located on the stack:

```
        args.rets = &args.args[be32_to_cpu(args.nargs)];
```

However args.nargs has not been range checked. That allows the guest to point args.rets anywhere up to +16GB from args.args.

The guest does not have control of what is written to args.rets, it is always (u32)-3, because subsequent code does check nargs. Additionally the guest will be killed as a result of the nargs being out of range, so a given guest only has a single shot at corrupting memory.

Only machines using Linux as the hypervisor, aka. KVM or bare metal, are affected by the bug.

The bug was introduced in:

```
    8e591cb72047 ("KVM: PPC: Book3S: Add infrastructure to implement kernel-side RTAS calls")
```

Which was first released in v3.10.

The upstream fix is:

```
  f62f3c20647e ("KVM: PPC: Book3S: Fix H_RTAS rets buffer overflow")

  https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=f62f3c20647ebd5fb6ecb8f0b477b9281c44c10a
```

Which will be included in the v5.14 release.

cheers

^ permalink raw reply    [**flat**|nested] 2+ messages in thread

---

```
* Re: Linux kernel: powerpc: KVM guest to host memory corruption
  2021-07-26  9:13 Linux kernel: powerpc: KVM guest to host memory corruption Michael Ellerman
@ 2021-07-27  0:46 ` Michael Ellerman
  0 siblings, 0 replies; 2+ messages in thread
From: Michael Ellerman @ 2021-07-27  0:46 UTC (permalink / raw)
  To: oss-security; +Cc: linuxppc-dev
```

Michael Ellerman <mpe@ellerman.id.au> writes:

> The Linux kernel for powerpc since v3.10 has a bug which allows a malicious KVM guest to corrupt host memory.
>
> In the handling of the H_RTAS hypercall, args.rets is made to point into the args.args buffer which is located on the stack:
>
> ```
>       args.rets = &args.args[be32_to_cpu(args.nargs)];
> ```
>
> However args.nargs has not been range checked. That allows the guest to point args.rets anywhere up to +16GB from args.args.
>
> The guest does not have control of what is written to args.rets, it is always (u32)-3, because subsequent code does check nargs. Additionally the guest will be killed as a result of the nargs being out of range, so a given guest only has a single shot at corrupting memory.
>
> Only machines using Linux as the hypervisor, aka. KVM or bare metal, are affected by the bug.
>
> The bug was introduced in:
>
> ```
>     8e591cb72047 ("KVM: PPC: Book3S: Add infrastructure to implement kernel-side RTAS calls")
> ```
>
> Which was first released in v3.10.
>
> The upstream fix is:
>
> ```
>   f62f3c20647e ("KVM: PPC: Book3S: Fix H_RTAS rets buffer overflow")
>
>   https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=f62f3c20647ebd5fb6ecb8f0b477b9281c44c10a
> ```
>
> Which will be included in the v5.14 release.

This has been assigned CVE-2021-37576.

cheers

^ permalink raw reply    [**flat**|nested] 2+ messages in thread

---

end of thread, other threads:[~2021-07-27  0:46 UTC | newest]

**Thread overview:** 2+ messages (download: mbox.gz / follow: Atom feed)
-- links below jump to the message on this page --

```
2021-07-26  9:13 Linux kernel: powerpc: KVM guest to host memory corruption Michael Ellerman
2021-07-27  0:46 ` Michael Ellerman
```

---