/tech/ - Technology★

Winner of the 61rd Attention-Hungry Games

/arda/ - For all things related to Middle Earth.

November 2018 - 8chan Transparency Report

Email	New Reply
Comment *	
File	Select/drop/paste files here
Password	f3fd4615e860€ (Randomized for file and post deletion; you may also set your own.)

* = required field

[▶ Show post options & limits]

Confused? See the FAQ.

Expand all images

Tree view

Enable gallery mode

File (hide): d6ecc681ccce18b….jpg (236.53 KB, 1280x960, 4:3, poettering.jpg) (h) (u)

[–] ▶ **ANOTHER SYSTEMD EXPLOIT** **Anonymous** 12/03/18 (Mon) 03:51:00 No.1004103>>1004174 [Watch Thread][Show All Posts]

UNPRIVILEGED USERS WITH UID > INT_MAX CAN SUCCESSFULLY EXECUTE ANY SYSTEMCTL COMMAND.

https://github.com/systemd/systemd/issues/11026

https://archive.is/73vP2

Anonymous 12/03/18 (Mon) 03:54:20 No.1004107>>1004110

it juts passes a password

Anonymous 12/03/18 (Mon) 04:03:05 No.1004110>>1004113 >>1004214

>>1004107

Pottering:

>it's the polkit service in the background that does the authentication. Not sure I grok what's going on, but this smells like a pokit service issue

Such a typical response.

Anonymous 12/03/18 (Mon) 04:13:11 No.1004113>>1004118

>>1004110

WTF does polkit even do? It's just one of those pieces of shitware that I habitually uninstall.

Anonymous 12/03/18 (Mon) 04:22:41 No.1004118>>1004127 >>1004145 >>1004239 >>1004291

>>1004113

It's to allow normal users to peform tasks that should normally require admin access.

http://smcv.pseudorandom.co.uk/2015/why_polkit/

Describes it well.

Anonymous 12/03/18 (Mon) 04:55:22 No.1004127

>>1004118

That's a good explanation, thanks.

I'm still not going to use it because I don't need such a thing, but at least I can understand why it exists.

Anonymous 12/03/18 (Mon) 06:36:04 No.1004145>>1004301

>>1004118

>not just using doas

Anonymous 12/03/18 (Mon) 08:05:10 No.1004174

>>1004103 (OP)

>UNPRIVILEGED USERS WITH UID > INT_MAX CAN SUCCESSFULLY EXECUTE ANY SYSTEMCTL COMMAND.

What is all this gibberish? Help me with my taskbar, it's disappeared. Obviously your fault since the last time I paid you to backup my video files.

Anonymous 12/03/18 (Mon) 08:43:12 No.1004191>>1004206 >>1004213

It's not an exploit per say, but it definietly goes to show how bad code quality is.

Anonymous 12/03/18 (Mon) 08:45:26 No.1004194>>1004199

>UID > INT_MAX

how does this ever happen

Anonymous 12/03/18 (Mon) 09:02:23 No.1004199

>>1004194

UID is a long, INT_MAX is an int.

Anonymous 12/03/18 (Mon) 09:19:47 No.1004206>>1004273 >>1004322 >>1004356

File (hide): 5300f6f14a509d7….jpg (1.79 MB, 1760x1322, 880:661, cathedral.jpg) (h) (u)

File (hide): abc41bfe68b565f….jpg (297.92 KB, 750x500, 3:2, bazaar.jpg) (h) (u)

>>1004191

Yep, and it's only going to get hugging worse.

Anonymous 12/03/18 (Mon) 09:55:31 No.1004213>>1004235

>>1004191

>per say

per se

Anonymous 12/03/18 (Mon) 09:55:50 No.1004214

>>1004110

I know,the bug should be fixed in system even though the bug is completely different software.

Anonymous 12/03/18 (Mon) 10:00:03 No.1004215>>1004216

It's a bug in policykit-1 and you need root privileges to create new users with custom UIDs anyway

Anonymous 12/03/18 (Mon) 10:01:50 No.1004216

>>1004215

this, it's not really an exploit.

It's just a really retarded bug.

Anonymous 12/03/18 (Mon) 11:30:09 No.1004227

>(((systemd)))

like poettering.

Anonymous 12/03/18 (Mon) 13:27:23 No.1004235

>>1004213

>per se

who the heck is perse

Anonymous 12/03/18 (Mon) 14:11:24 No.1004239

>>1004118

Basically it's useless shit for "year of the Leenoox danktop" cunts who can't into sudo or just su to root or login as root on /dev/ttyX. Those subversive bastards can go get notabuggered into oblivion for all I care.

Anonymous 12/03/18 (Mon) 14:42:59 No.1004243>>1004253 >>1004271 >>1004274 >>1004317 >>1004339

>ANOTHER SYSTEMD EXPLOIT

>UNPRIVILEGED USERS WITH UID > INT_MAX

More like another C integer overflow bug.

Why am I retraining myself in Ada? Because since 1979 I have been trying to write reliable code in C. (Definition: reliable code never gives wrong answers without an explicit apology.) Trying and failing. I have been frustrated to the screaming point by trying to write code that could survive (some) run-time errors in other people's code linked with it. I'd look wistfully at BSD's three-argument signal handlers, which at least offered the possibility of provide hardware specific recovery code in #ifdefs, but grit my teeth and struggle on having to write code that would work in System V as well.

There are times when I feel that clocks are running faster but the calendar is running backwards. My first serious programming was done in Burroughs B6700 Extended Algol. I got used to the idea that if the hardware can't give you the right answer, it complains, and your ON OVERFLOW statement has a chance to do something else. That saved my bacon more than once.

When I met C, it was obviously pathetic compared with the _real_ languages I'd used, but heck, it ran on a 16-bit machine, and it was better than 'as'. When the VAX came out, I was very pleased: "the interrupt on integer overflow bit is _just_ what I want". Then I was very disappointed: "the wretched C system _has_ a signal for integer overflow but makes sure it never happens even when it ought to".

It would be a good thing if hardware designers would remember that the ANSI C standard provides _two_ forms of "integer" arithmetic: 'unsigned' arithmetic which must wrap around, and 'signed' arithmetic which MAY TRAP (or wrap, or make demons fly out of your nose). "Portable C programmers", know that they CANNOT rely on integer arithmetic _not_ trapping, and they know (if they have done their homework) that there are commercially significant machines where C integer overflow _is_ trapped, so they would rather the Alpha trapped so that they could use the Alpha as a porting base.

Having said which: I will gladly put up with the Alpha exception mechanism as long as

- there is a documented C-callable function which controls the integer trapping state
- there is a documented C-callable function which controls IEEE-ish floating-point traps
- there is a documented C-callable function which includes a barrier (can I _rely_ on signal(SIGFPE, f) including a barrier?)

▶ **Anonymous** 12/03/18 (Mon) 14:51:11 No.1004246>>1004295

File (hide): 26cc831e2d8e3e4….jpg (2.71 MB, 3456x2304, 3:2, poter-ring.jpg) (h) (u)

ITT : post le poitering face

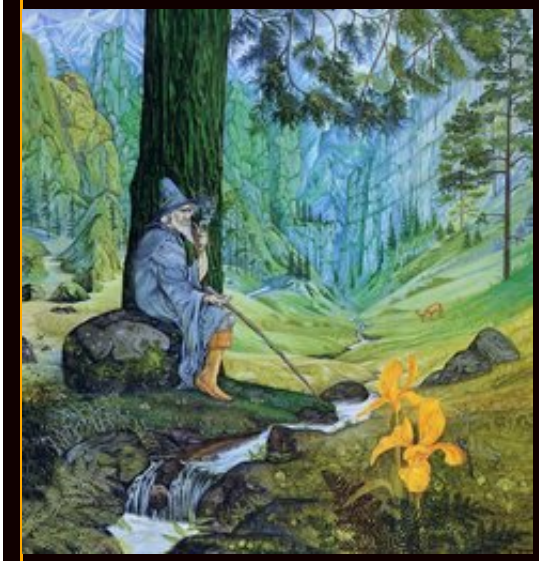
▶ **Anonymous** 12/03/18 (Mon) 15:13:50 No.1004253>>1004302 >>1004339

>>1004243

That long quote is against you, retard. C did nothing but try to consider all the possible hardware, including the retarded archs.

▶ **Anonymous** 12/03/18 (Mon) 16:51:12 No.1004271>>1004302 >>1004312 >>1004339

File (hide): 882f978c4d407af….jpg (403.5 KB, 1174x1250, 587:625, 982a9960.jpg) (h) (u)



>>1004243

C is a powerful tool. Much like a mere peasant couldn't properly wield a zweihänder, only causing injury to himself. You need to have gains from the gym of software security and computer logic in order to wield C to horse-slicing epicness. With C YOU are the person penetrating into the backside of your computer, you need to assert dominance and have the proper skills to keep the slave in line or it might cause total financial ruin on you.

Pray to the apostles of electrical manipulation: Dennis, Ken and Brian.

▶ **Anonymous** 12/03/18 (Mon) 17:17:24 No.1004273

>>1004206

You spelled Brazzer wrong.

Anonymous 12/03/18 (Mon) 17:19:12 No.1004274>>1004339

>>1004243

I support C. You hipsters can get hugged.

Anonymous 12/03/18 (Mon) 18:26:28 No.1004291

>>1004118

So create a semi-privileged group and give them permission to use sudo for that particular task.

Anonymous 12/03/18 (Mon) 18:50:01 No.1004295

>>1004246

If Pottering released his own OS, I'd unironically use it over Linux.

>There is a bug, but it lies with the firmware

>Issue closed [willnotfix]

Anonymous 12/03/18 (Mon) 18:56:24 No.1004298

>UID > INT_MAX CAN

How feasible is that? Is this the same bullshit about users that start/contain numbers and would never happen anyway?

Anonymous 12/03/18 (Mon) 19:10:26 No.1004301

>>1004145

I believe polkit(Policy Kit) is to configure what users can and can't do rather than passing a privilege escalation program such as sudo or doas in the shell.

Your comment only would have made sense had this been a discussion about sudo.

Anonymous 12/03/18 (Mon) 19:11:21 No.1004302>>1004307 >>1004339

>>1004253

Even on non-retarded hardware that has trapping instructions or lets you set a trap on overflow bit, there is nothing you can do to recover from the error. Ada has to check for overflows and raise an exception no matter what the hardware does unless you suppress overflow checks. C did not consider most of the hardware Ada and other non-UNIX languages can run on at all. UNIX has even more hardware restrictions than C, which is why all these RISCs are just 64-bit clones of the PDP-11 with its flat address space.

>>1004271

>C is a powerful tool.

C weenies always call C powerful but all they mean is that C has pointer arithmetic. You can't write malloc or a GC in standard C. What you can do in standard C without undefined behavior is a lot more restricted and less useful than most languages.

>Much like a mere peasant couldn't properly wield a zweihänder, only causing injury to himself.

You need to have gains from the gym of software security and computer logic in order to wield C to horse-slicing epicness.

Why do none of the Linux or systemd "programmers" have these "gains" or "horse-slicing epicness" or whatever you want to call it? They are the ones responsible for all these bugs and exploits, but that's not surprising since the C language itself is just as buggy and defective as C code.

https://en.wikipedia.org/wiki/C18_(C_standard_revision)

>C18 addressed defects in C11 without introducing new language features.[3]

>The STDC_VERSION macro is increased to the value 201710L.

The C standards committee made a language with so many "defects" that the only "new feature" in 7 years was a new version number. If it was any other language (even C++), this would be a joke and probably the end of the standards committee, but in the C community, the only thing surprising about taking 7 years just to fix bugs in the standard is that it didn't take longer.

>With C YOU are the person penetrating into the backside of your computer, you need to assert dominance

With C, 15,600 Linux weenies are "penetrating into the backside of your computer," not including EFI, X11, and all that other C bullshit. You have no control because C needs so much code to do anything. Your "Hello World" and "FizzBuzz" might seem "powerful" and "dominant" to you, but it's nothing compared to the more than 60 million lines of C and C++ code you need just to be able to post here. Lisp machines have created a better environment with much less code.

>and have the proper skills to keep the slave in line or it might cause total financial ruin on you.

Just like what happened to Lucent, SGI, and all these other UNIX companies, and all these C projects like Workplace OS and Copland.

>Pray to the apostles of electrical manipulation: Dennis, Ken and Brian.

I have a lot of respect for "apostles of electrical manipulation" who created computer systems and subsystems. These AT&T employees were just shitty "programmers" who were not smart enough to do system calls properly or make a compiler that could check array bounds or integer overflows, and then blamed the hardware for their own inabilities. Much like outsourced Pajeet code, "their" pile of shit was only used to save money on licensing fees and to avoid hiring real programmers, and most of it had to be replaced and was written by other people anyway.

> **Subject**: Mixed Up Mail
>
> I cannot think of a comment to add that could possibly top what follows.
>
> I can. Isn't it typical that unix weenies would blame hardware for this problem? Can you imagine a hardware fault that would explain this snafu? Not a chance. This is the Great Satan Sendmail feeding its dark energy on the mail files of innocents.

▶ **Anonymous** 12/03/18 (Mon) 19:42:09 No.1004307>>1004310 >>1004339

>>1004302

shoo shoo

sudo apt-get remove rust* libstd-rust* cargo*

sudo apt-get remove snapd* libsnapd*

▶ **Anonymous** 12/03/18 (Mon) 19:47:32 No.1004310>>1004339

>>1004307

you're a retard and devalue any thread you post in. I'd rather have you banned than the LARPer you're responding to.

Anonymous 12/03/18 (Mon) 19:51:37 No.1004312

>>1004271

Kernighan has done nothing of note except awk, and to act as a UNIX talking head. Stop idolising C. It's good but it's not this magic wondertool that only works in the hands of mega-geniuses; you're simply consistently writing trivial programs

Anonymous 12/03/18 (Mon) 20:02:44 No.1004317

>>1004243

based

Anonymous 12/03/18 (Mon) 20:10:52 No.1004322

>>1004206

Ha! A cathedral and bazaar reference.

Anonymous 12/03/18 (Mon) 21:48:47 No.1004339

>>1004243

>>1004253

>>1004271

>>1004274

>>1004302

>>1004307

>>1004310

>>>/metatech/1855

sage for offtopic

Anonymous 12/03/18 (Mon) 22:34:48 No.1004352

File (hide): 85eee9c578fd227….png (841.69 KB, 1024x678, 512:339, todd poettering.png) (h) (u)

It just works.

Anonymous 12/03/18 (Mon) 22:42:34 No.1004356>>1004358 >>1004359

>>1004206

What are those pictures of?

Anonymous 12/03/18 (Mon) 22:44:11 No.1004358

>>1004356

The first is a cathedral, the second is a bazaar.

Anonymous 12/03/18 (Mon) 22:52:14 No.1004359

>>1004356

Lurk 2 years before posting.

Anonymous 12/04/18 (Tue) 00:31:45 No.1004371>>1004406

Bump, how will Lennart ever recover? It's pretty clear that System D is full of these exploits and it's likely three are committed to the codebase for every one squashed.

Anonymous 12/04/18 (Tue) 01:36:02 No.1004378>>1004449

>tfw using ***OpenBSD***

Anonymous 12/04/18 (Tue) 03:10:46 No.1004406>>1004816

>>1004371

No it's not clear. If you have a report detailing your numbers, then that will clear it up.

Anonymous 12/04/18 (Tue) 05:59:36 No.1004449>>1004665

>>1004378

Enjoy while it lasts. Look at what people are OBSD and look at their twatters. You know, Theo can

get fucked like Linus easily. Especially now when many refugess must have spread the word.

Anonymous 12/04/18 (Tue) 16:47:10 No.1004665>>1004816

>>1004449

OpenBSD isn't owned by commercial interests, so it's not vulnerable to the same shenanigans. They would have better luck to pwn NetBSD but even there they have enough redpilled people who resist.

Then there's the fact that it would largely be a wasted effort. Not enough people run those OS for it to matter. They don't try to provide an alternative to Windows with the "year of the Leenoox danktop" shit, where everything has to be something idiot can click on, instead of reading man page and understanding how the OS works fundamentally.

Anonymous 12/04/18 (Tue) 23:17:00 No.1004816

>>1004406

>I need a "report detailing my numbers" to know what's plainly evident

>>1004665

The biggest NetBSD installation is the non-profit sdf.org and developers of the OS are involved with that organization. It's typically running any upgrade long before the official release. They will take good care of it. SDF might be the last wild west multi-user Unix system community.
