basealt.ru

ООО «Базальт СПО»

Российский разработчик
операционных систем «Альт»

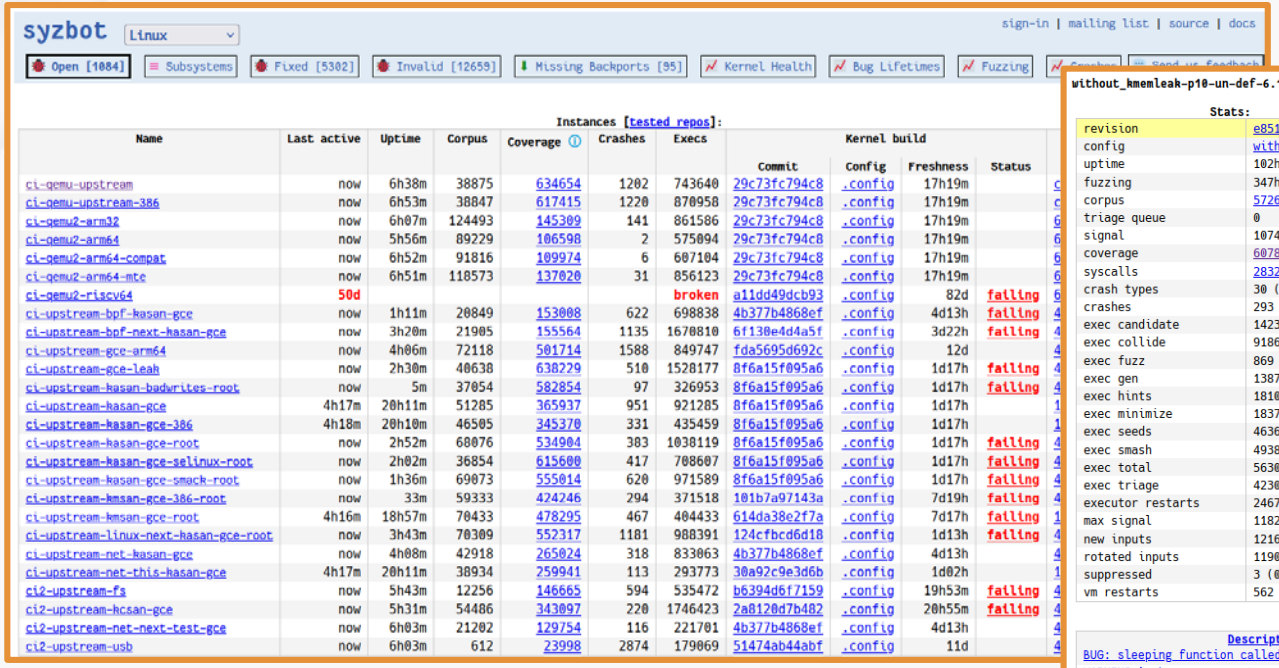
Опыт взаимодействия с международным сообществом разработчиков при исправлении уязвимостей: ответственное разглашение, сроки исправления

Егор Игнатов egori@basealt.ru
Александр Кузнецов kuznetsovam@basealt.ru
Александр Шашкин dutyrok@basealt.ru

Взаимодействие с международным сообществом разработчиков ядра Linux

На примере срабатывания
WARNING in vmci_datagram_dispatch

Фаззинг ядра Linux



syzbot Linux

sign-in | mailing list | source | docs

Open [1084] | Subsystems | Fixed [5302] | Invalid [12659] | Missing Backports [95] | Kernel Health | Bug Lifetimes | Fuzzing | Crashes | Send us feedback

Instances [tested repos]:

Name	Last active	Uptime	Corpus	Coverage	Crashes	Execs	Kernel build				
							Commit	Config	Freshness	Status	
ci-qemu-upstream	now	6h38m	38875	634654	1202	743640	29c73fc794c8	.config	17h19m		c
ci-qemu-upstream-386	now	6h53m	38847	617415	1220	870958	29c73fc794c8	.config	17h19m		c
ci-qemu2-arm32	now	6h07m	124493	145309	141	861586	29c73fc794c8	.config	17h19m		6
ci-qemu2-arm64	now	5h56m	89229	106598	2	575094	29c73fc794c8	.config	17h19m		6
ci-qemu2-arm64-compat	now	6h52m	91816	109974	6	607104	29c73fc794c8	.config	17h19m		6
ci-qemu2-arm64-mte	now	6h51m	118573	137020	31	856123	29c73fc794c8	.config	17h19m		6
ci-qemu2-riscv64	50d					broken	a11dd49dcb93	.config	82d	failing	6
ci-upstream-bpf-kasan-gce	now	1h11m	20849	153008	622	698838	4b377b4868ef	.config	4d13h	failing	4
ci-upstream-bpf-next-kasan-gce	now	3h20m	21905	155564	1135	1670810	6f130e4d4a5f	.config	3d22h	failing	4
ci-upstream-gce-arm64	now	4h06m	72118	501714	1588	849747	fda5695d692c	.config	12d		4
ci-upstream-gce-leak	now	2h30m	40638	638229	510	1528177	8f6a15f095a6	.config	1d17h	failing	4
ci-upstream-kasan-badwrites-root	now	5m	37054	582854	97	326953	8f6a15f095a6	.config	1d17h	failing	4
ci-upstream-kasan-gce	4h17m	20h11m	51285	365937	951	921285	8f6a15f095a6	.config	1d17h		1
ci-upstream-kasan-gce-386	4h18m	20h10m	46505	345370	331	435459	8f6a15f095a6	.config	1d17h		1
ci-upstream-kasan-gce-root	now	2h52m	68076	534904	383	1038119	8f6a15f095a6	.config	1d17h	failing	4
ci-upstream-kasan-gce-selinux-root	now	2h02m	36854	615600	417	708607	8f6a15f095a6	.config	1d17h	failing	4
ci-upstream-kasan-gce-smack-root	now	1h36m	69073	555014	620	971589	8f6a15f095a6	.config	1d17h	failing	4
ci-upstream-kmsan-gce-386-root	now	33m	59333	424246	294	371518	101b7a97143a	.config	7d19h	failing	4
ci-upstream-kmsan-gce-root	4h16m	18h57m	70433	478295	467	404433	614da38e2f7a	.config	7d17h	failing	1
ci-upstream-linux-next-kasan-gce-root	now	3h43m	70309	552317	1181	988391	124cfbcd6d18	.config	1d13h	failing	4
ci-upstream-net-kasan-gce	now	4h08m	42918	265024	318	833063	4b377b4868ef	.config	4d13h		4
ci-upstream-net-this-kasan-gce	4h17m	20h11m	38934	259941	113	293773	30a92c9e3d6b	.config	1d02h		1
ci2-upstream-fs	now	5h43m	12256	146665	594	535472	b6394d6f7159	.config	19h53m	failing	4
ci2-upstream-kcsan-gce	now	5h31m	54486	343097	220	1746423	2a8120d7b482	.config	20h55m	failing	4
ci2-upstream-net-next-test-gce	now	6h03m	21202	129754	116	221701	4b377b4868ef	.config	4d13h		4
ci2-upstream-usb	now	6h03m	612	23998	2874	179069	51474ab44abf	.config	11d		4

without_kmemleak-p10-un-def-6.1.79-alt0.c10f.2 syzkaller

Stats:

revision	e851e4c1
config	without_kmemleak-…
uptime	102h14m47s
fuzzing	347h44m0s
corpus	572631
triage queue	0
signal	10746772
coverage	6078064
syscalls	2832
crash types	30 (0/hour)
crashes	293 (2/hour)
exec candidate	1423914 (232/min)
exec collide	9186239 (24/sec)
exec fuzz	869 (8/hour)
exec gen	1387 (13/hour)
exec hints	18105713 (49/sec)
exec minimize	18373793 (49/sec)
exec seeds	46369 (453/hour)
exec smash	4938025 (13/sec)
exec total	56307025 (153/sec)
exec triage	4230852 (11/sec)
executor restarts	2467 (24/hour)
max signal	11824432 (32/sec)
new inputs	1216806 (198/min)
rotated inputs	119012 (19/min)
suppressed	3 (0/hour)
vm restarts	562 (5/hour)

Crashes:

Description	Count	Last Time	Report
BUG: sleeping function called from invalid context i…	100	2024/03/29 16:09	has C repro
WARNING in kvm_vcpu_reset	100	2024/03/29 15:17	has C repro
INFO: rcu detected stall in perf_event_open	5	2024/03/29 12:13	has C repro
WARNING in __floppy_read_block_0	100	2024/03/29 06:35	has C repro
suppressed report	100	2024/03/29 03:56	
WARNING in vmci_datagram_dispatch	19	2024/03/29 02:19	has C repro
WARNING: suspicious RCU usage in sta_remove_link	12	2024/03/28 23:36	has repro
SYZFATAL: Manager.NewInput call failed: read tcp IP:…	23	2024/03/28 18:38	non-reproducible
INFO: rcu detected stall in corrupted	24	2024/03/28 18:08	
WARNING in floppy_interrupt	16	2024/03/28 14:49	has C repro
unregister_netdevice: waiting for DEV to become free	3	2024/03/28 00:48	has C repro
INFO: rcu detected stall in syscall_exit_to_user_mode	3	2024/03/27 10:12	non-reproducible

Рассматриваемое срабатывание

WARNING in vmci_datagram_dispatch

Исправлено 08.03.2024

WARNING in vmci_datagram_dispatch

Исправление срабатывания

```
diff --git a/drivers/misc/vmw_vmci/vmci_datagram.c b/drivers/misc/vmw_vmci/vmci_datagram.c
index f50d22882476f9..27853b31e288b1 100644
--- a/drivers/misc/vmw_vmci/vmci_datagram.c
+++ b/drivers/misc/vmw_vmci/vmci_datagram.c
@@ -234,7 +234,10 @@ static int dg_dispatch_as_host(u32 context_id, struct vmci_datagram *dg)

                dg_info->in_dg_host_queue = true;
                dg_info->entry = dst_entry;
-               memcpy(&dg_info->msg, dg, dg_size);
+               memcpy(&dg_info->msg, dg, VMCI_DG_HEADERSIZE);
+               if (dg->payload_size) {
+                       memcpy(dg_info->msg_payload, VMCI_DG_PAYLOAD(dg), dg->payload_size);
+               }

                INIT_WORK(&dg_info->work, dg_delayed_dispatch);
                schedule_work(&dg_info->work);
@@ -377,7 +380,10 @@ int vmci_datagram_invoke_guest_handler(struct vmci_datagram *dg)

        dg_info->in_dg_host_queue = false;
        dg_info->entry = dst_entry;
-       memcpy(&dg_info->msg, dg, VMCI_DG_SIZE(dg));
+       memcpy(&dg_info->msg, dg, VMCI_DG_HEADERSIZE);
+       if (dg->payload_size) {
+               memcpy(dg_info->msg_payload, VMCI_DG_PAYLOAD(dg), dg->payload_size);
+       }

        INIT_WORK(&dg_info->work, dg_delayed_dispatch);
        schedule_work(&dg_info->work);
--
```

drivers/misc/vmw_vmci/vmci_datagram.c

Руководство по отправке исправлений

Essential guide

Submitting patches: the essential guide to getting your code into the kernel ¶

English

For a person or company who wishes to submit a change to the Linux kernel, the process can sometimes be daunting if you're not familiar with "the system." This text is a collection of suggestions which can greatly increase the chances of your change being accepted.

Submit patches to -stable tree

Procedure for submitting patches to the -stable tree ¶

Note:

Security patches should not be handled (solely) by the -stable review process but should follow the procedures in Documentation/process/security-bugs.rst.

Трудности общения с сообществом

From Linus Torvalds <>
Date Fri, 26 Jan 2024 12:25:05 -0800
Subject Re: [PATCH] eventfs: Have inodes have unique inode numbers

Steven,
stop making things more complicated than they need to be.

And dammit, STOP COPYING VFS LAYER FUNCTIONS.

It was a bad idea last time, it's a horribly bad idea this time too.
[...]

Src: [lore.kernel.org]

WARNING in vmci_datagram_dispatch

Хронология событий

27.12.2023 — Письмо мейнтейнерам драйвера VMware VMCI

WARNING in vmci_datagram_dispatch

Отправка изменений

```
linux-kernel.vger.kernel.org archive mirror
                          search help / color / mirror / Atom feed

* [PATCH 0/1] misc/vmw_vmci: fix filling of the msg and msg_payload in dg_info struct
@ 2024-01-10 10:40 kovalev
  2024-01-10 10:40 ` [PATCH 1/1] " kovalev
  2024-01-10 10:53 ` [PATCH 0/1] " Greg KH
  0 siblings, 2 replies; 6+ messages in thread
From: kovalev @ 2024-01-10 10:40 UTC (permalink / raw)
  To: bryantan, vdasa, pv-drivers, arnd, gregkh, linux-kernel
  Cc: kovalev, nickel, oficerovas, dutyrok

Warning detected by tracking mechanisms __fortify_memcpy_chk, added 2021-04-20.
The proposed patch (PATCH 1/1) introduces changes to meet the new requirements.

The reproducer (repro.c) was generated using the syzkaller program and minimized
(Thanks Alexander Ofitserov <oficerovas@altlinux.org>):
```

Src: [submit patches to upstream]

WARNING in vmci_datagram_dispatch

Хронология событий

27.12.2023 — Письмо мейнтейнерам драйвера VMware VMCI

10.01.2024 — Повторная отправка исправления с указанием адреса рассылки

WARNING in vmci_datagram_dispatch

Хронология событий

27.12.2023	Письмо мейнтейнерам драйвера VMware VMCI
05.01.2024	**Исправление этой же ошибки отправлено компанией Oracle**
10.01.2024	Повторная отправка исправления с указанием адреса рассылки
10.01.2024	**Ответ о том, что компания Oracle присылала подобные изменения**

WARNING in vmci_datagram_dispatch

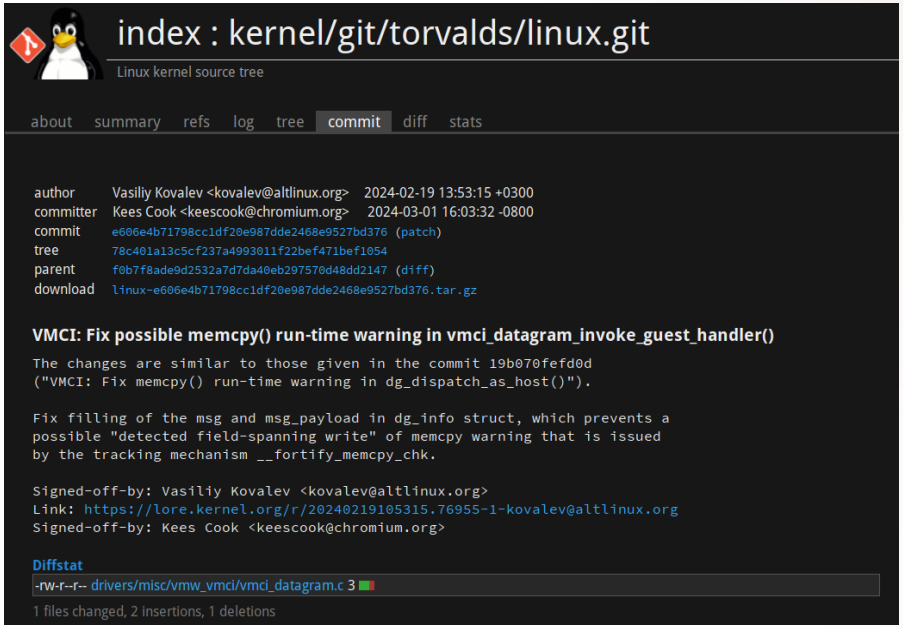
Исправление срабатывания

```
diff --git a/drivers/misc/vmw_vmci/vmci_datagram.c b/drivers/misc/vmw_vmci/vmci_datagram.c
index f50d22882476f9..27853b31e288b1 100644
--- a/drivers/misc/vmw_vmci/vmci_datagram.c
+++ b/drivers/misc/vmw_vmci/vmci_datagram.c
@@ -234,7 +234,10 @@ static int dg_dispatch_as_host(u32 context_id, struct vmci_datagram *dg)

                dg_info->in_dg_host_queue = true;
                dg_info->entry = dst_entry;
-               memcpy(&dg_info->msg, dg, dg_size);
+               memcpy(&dg_info->msg, dg, VMCI_DG_HEADERSIZE);
+               if (dg->payload_size) {
+                       memcpy(dg_info->msg_payload, VMCI_DG_PAYLOAD(dg), dg->payload_size);
+               }

                INIT_WORK(&dg_info->work, dg_delayed_dispatch);
                schedule_work(&dg_info->work);
@@ -377,7 +380,10 @@ int vmci_datagram_invoke_guest_handler(struct vmci_datagram *dg)

        dg_info->in_dg_host_queue = false;
        dg_info->entry = dst_entry;
-       memcpy(&dg_info->msg, dg, VMCI_DG_SIZE(dg));
+       memcpy(&dg_info->msg, dg, VMCI_DG_HEADERSIZE);
+       if (dg->payload_size) {
+               memcpy(dg_info->msg_payload, VMCI_DG_PAYLOAD(dg), dg->payload_size);
+       }

        INIT_WORK(&dg_info->work, dg_delayed_dispatch);
        schedule_work(&dg_info->work);
--
```

drivers/misc/vmw_vmci/vmci_datagram.c

WARNING in vmci_datagram_dispatch

Исправление аналогичной проблемы



index : kernel/git/torvalds/linux.git

Linux kernel source tree

about summary refs log tree commit diff stats

author Vasiliy Kovalev <kovalev@altlinux.org> 2024-02-19 13:53:15 +0300
committer Kees Cook <keescook@chromium.org> 2024-03-01 16:03:32 -0800
commit e606e4b71798cc1df20e987dde2468e9527bd376 (patch)
tree 78c401a13c5cf237a4993011f22bef471bef1054
parent f0b7f8ade9d2532a7d7da40eb297570d48dd2147 (diff)
download linux-e606e4b71798cc1df20e987dde2468e9527bd376.tar.gz

VMCI: Fix possible memcpy() run-time warning in vmci_datagram_invoke_guest_handler()

The changes are similar to those given in the commit 19b070fefd0d
("VMCI: Fix memcpy() run-time warning in dg_dispatch_as_host()").

Fix filling of the msg and msg_payload in dg_info struct, which prevents a
possible "detected field-spanning write" of memcpy warning that is issued
by the tracking mechanism __fortify_memcpy_chk.

Signed-off-by: Vasiliy Kovalev <kovalev@altlinux.org>
Link: https://lore.kernel.org/r/20240219105315.76955-1-kovalev@altlinux.org
Signed-off-by: Kees Cook <keescook@chromium.org>

Diffstat

-rw-r--r-- drivers/misc/vmw_vmci/vmci_datagram.c 3

1 files changed, 2 insertions, 1 deletions

Src: upstream commit

WARNING in vmci_datagram_dispatch

Хронология событий

27.12.2023	Письмо мейнтейнерам драйвера VMware VMCI
05.01.2024	Исправление этой же ошибки отправлено компанией Oracle
10.01.2024	Повторная отправка исправления с указанием адреса рассылки
10.01.2024	Ответ о том, что компания Oracle присылала подобные изменения
19.02.2024	Отправлены исправления для аналогичной проблемы

WARNING in vmci_datagram_dispatch

Хронология событий

27.12.2023	Письмо мейнтейнерам драйвера VMware VMCI
05.01.2024	Исправление этой же ошибки отправлено компанией Oracle
10.01.2024	Повторная отправка исправления с указанием адреса рассылки
10.01.2024	Ответ о том, что компания Oracle присылала подобные изменения
19.02.2024	Отправлены исправления для аналогичной проблемы
08.03.2024	Изменения приняты в основную ветку ядра

Извлеченные уроки

1

Четко следовать процедуре ответственного разглашения, определенной для конкретного программного обеспечения

2

3

Взаимодействие с международным сообществом разработчиков прокси-сервера Squid

На примере уязвимости
CVE-2023-46848

Рассматриваемая уязвимость

CVE-2023-46848

DoS: CWE-193: Incorrect conversion between Numeric types

Severity: 8.6 (high)

Исправлено
21.10.2023

CVE-2023-46848

Хронология событий

05.05.2023	Письмо в закрытый список рассылки

CVE-2023-46848

Хронология событий

05.05.2023	Письмо в закрытый список рассылки
08.05.2023	Закрытое подтверждение уязвимости

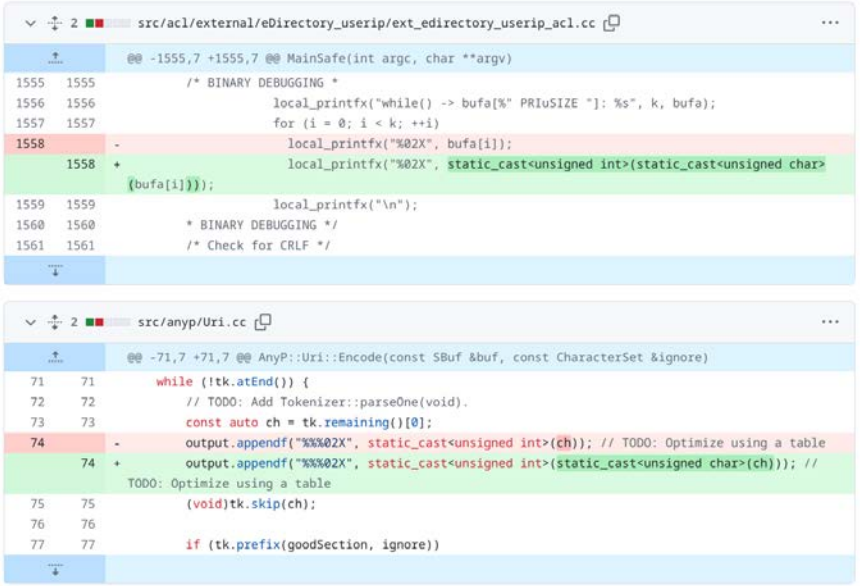
CVE-2023-46848

Хронология событий

05.05.2023	Письмо в закрытый список рассылки
08.05.2023	Закрытое подтверждение уязвимости
27.05.2023	Закрытое исправление

CVE-2023-46848

Исправление уязвимости



2 src/acl/external/eDirectory_userip/ext_edirectory_userip_acl.cc

```
@@ -1555,7 +1555,7 @@ MainSafe(int argc, char **argv)
1555 1555          /* BINARY DEBUGGING *
1556 1556                      local_printfx("while() -> bufa[%" PRIuSIZE "]: %s", k, bufa);
1557 1557                      for (i = 0; i < k; ++i)
1558      -                        local_printfx("%02X", bufa[i]);
     1558 +                        local_printfx("%02X", static_cast<unsigned int>(static_cast<unsigned char>(bufa[i])));
1559 1559                      local_printfx("\n");
1560 1560          * BINARY DEBUGGING */
1561 1561          /* Check for CRLF */
```

2 src/anyp/Uri.cc

```
@@ -71,7 +71,7 @@ AnyP::Uri::Encode(const SBuf &buf, const CharacterSet &ignore)
71 71      while (!tk.atEnd()) {
72 72          // TODO: Add Tokenizer::parseOne(void).
73 73          const auto ch = tk.remaining()[0];
74      -        output.appendf("%%%02X", static_cast<unsigned int>(ch)); // TODO: Optimize using a table
   74 +        output.appendf("%%%02X", static_cast<unsigned int>(static_cast<unsigned char>(ch))); // TODO: Optimize using a table
75 75          (void)tk.skip(ch);
76 76
77 77          if (tk.prefix(goodSection, ignore))
```

[src/acl/external/eDirectory_userip/ext_edirectory_userip_acl.cc]

CVE-2023-46848

Хронология событий

05.05.2023	Письмо в закрытый список рассылки
08.05.2023	Закрытое подтверждение уязвимости
27.05.2023	Закрытое исправление
21.10.2023	Публичное раскрытие (релиз с исправлением)

CVE-2023-46848

Публикация информации

Credits:

This vulnerability was discovered by Joshua Rogers of Opera Software.

Revision history:

2023-10-12 11:53:02 UTC Initial Report

Src: SQUID-2023:5 GHSA

Извлеченные уроки

1

Четко следовать процедуре ответственного разглашения, определенной для конкретного программного обеспечения

2

Самостоятельно устанавливать период эмбарго на неразглашение информации об уязвимости

3

Взаимодействие с международным сообществом разработчиков библиотеки Libvirt

На примере уязвимостей
CVE-2024-1441 и CVE-2024-2494

Рассматриваемые уязвимости

CVE-2024-1441

DoS: CWE-193:
Off-by-one Error

Severity: 5.5 (medium)

Исправлено
01.03.2024

CVE-2024-2494

DoS: CWE-789: Memory Allocation with Excessive Size Value

Severity: 6.2 (medium)

Исправлено
21.03.2024

CVE-2024-1441

Исправление уязвимости

src/interface/interface_backend_udev.c +1 −1

```
...  ...  @@ -222,7 +222,7 @@ udevListInterfacesByStatus(virConnectPtr conn,
222  222          g_autoptr(virInterfaceDef) def = NULL;
223  223
224  224          /* Ensure we won't exceed the size of our array */
225       -      if (count > names_len)
     225  +      if (count >= names_len)
226  226              break;
227  227
228  228          path = udev_list_entry_get_name(dev_entry);
...  ...
```

src/interface/interface_backend_udev.c

CVE-2024-1441

Сроки разглашения

«This bug is subject to a 90 day disclosure deadline. If a fix for this issue is made available to users before the end of the 90-day deadline, this bug report will become public 30 days after the fix was made available. Otherwise, this bug report will become public at the deadline.»

Src: [Project Zero Vulnerability Disclosure FAQ]

CVE-2024-1441

Хронология событий

09.02.2024 — Письмо в закрытый список рассылки с эмбарго 90 дней

CVE-2024-1441

Хронология событий

09.02.2024 — Письмо в закрытый список рассылки с эмбарго 90 дней

12.02.2024 — Закрытое присвоение CVE

CVE-2024-1441

Хронология событий

09.02.2024 — Письмо в закрытый список рассылки с эмбарго 90 дней

12.02.2024 — Закрытое присвоение CVE

01.03.2024 — Публичное раскрытие (коммит в мастер-ветку)

CVE-2024-2494

Исправление уязвимости

src/remote/remote_daemon_dispatch.c +65 −0 View file @ 8a3f8d95

```
...  ...  @@ -2497,6 +2505,10 @@ remoteDispatchDomainBlockStatsFlags(virNetServer *server G_GNUC_UNUSED,
2497 2505          goto cleanup;
2498 2506      flags = args->flags;
2499 2507
     2508 +    if (args->nparams < 0) {
     2509 +        virReportError(VIR_ERR_INTERNAL_ERROR, "%s", _("nparams must be non-negative"));
     2510 +        goto cleanup;
     2511 +    }
2500 2512      if (args->nparams > REMOTE_DOMAIN_BLOCK_STATS_PARAMETERS_MAX) {
2501 2513          virReportError(VIR_ERR_INTERNAL_ERROR, "%s", _("nparams too large"));
2502 2514          goto cleanup;
...  ...  @@ -2717,6 +2729,14 @@ remoteDispatchDomainGetVcpuPinInfo(virNetServer *server G_GNUC_UNUSED,
```

```
2516      if (args->nparams)
2517          params = g_new0(virTypedParameter, args->nparams);
2518      nparams = args->nparams;
```

[src/remote/remote_daemon_dispatch.c]

CVE-2024-2494

Сроки разглашения

The general aim of the team is to have embargo dates which are **two weeks or less in duration**. [...] In exceptional circumstances longer initial embargoes may be negotiated by mutual agreement [...]. Any such extended embargoes will aim to be **at most one month in duration**.

Src: [Libvirt Security Process]

CVE-2024-2494

Хронология событий

01.03.2024 — Письмо в закрытый список рассылки с эмбарго 14 дней

CVE-2024-2494

Хронология событий

01.03.2024 — Письмо в закрытый список рассылки с эмбарго 14 дней

06.03.2024 — Закрытое обсуждение исправлений

CVE-2024-2494

Хронология событий

01.03.2024	Письмо в закрытый список рассылки с эмбарго 14 дней
06.03.2024	Закрытое обсуждение исправлений
14.03.2024	Напоминание об истечении периода эмбарго

CVE-2024-2494

Хронология событий

01.03.2024	Письмо в закрытый список рассылки с эмбарго 14 дней
06.03.2024	Закрытое обсуждение исправлений
14.03.2024	Напоминание об истечении периода эмбарго
15.03.2024	Закрытое присвоение CVE

CVE-2024-2494

Хронология событий

01.03.2024	Письмо в закрытый список рассылки с эмбарго 14 дней
06.03.2024	Закрытое обсуждение исправлений
14.03.2024	Напоминание об истечении периода эмбарго
15.03.2024	Закрытое присвоение CVE
18.03.2024	Договоренность о раскрытии через 2 дня

CVE-2024-2494

Хронология событий

01.03.2024	Письмо в закрытый список рассылки с эмбарго 14 дней
06.03.2024	Закрытое обсуждение исправлений
14.03.2024	Напоминание об истечении периода эмбарго
15.03.2024	Закрытое присвоение CVE
18.03.2024	Договоренность о раскрытии через 2 дня
21.03.2024	Публичное раскрытие (публикация в devel-рассылке)

Извлеченные уроки

1

Четко следовать процедуре ответственного разглашения, определенной для конкретного программного обеспечения

2

Самостоятельно устанавливать период эмбарго на неразглашение информации об уязвимости

3

Заранее определять и информировать разработчиков о порядке действий в случае истечения периода эмбарго. Периодически обозначать приближающееся истечение периода эмбарго

Контакты:

Тел.: +7 (495) 123-47-99

E-mail: contact@basealt.ru

Бесплатная техническая
поддержка на этапе
тестирования:
basealt.ru/sales2

Офисы:

Москва, ул. Бутырская, д. 75

Санкт-Петербург, 4-я линия В.О., д. 17, БЦ «ЛВА»

Саратов, ул. Октябрьская 44, корпус А, офис № 3

Обнинск, ул. Королёва, д. 4Б, БЦ “Британика”

Казань, ул. Петербургская, д. 50, корп. 5, офис №422

www.basealt.ru

basealt.ru

ООО «Базальт СПО»

Российский разработчик
операционных систем «Альт»

Опыт взаимодействия с международным сообществом разработчиков при исправлении уязвимостей: ответственное разглашение, сроки исправления

Егор Игнатов egori@basealt.ru
Александр Кузнецов kuznetsovam@basealt.ru
Александр Шашкин dutyrok@basealt.ru