Kernel Live Patch Security Notice LSN-0082-1

Authored by Benjamin M. Romer

Posted Nov 12, 2021

Jann Horn discovered that the tty subsystem of the Linux kernel did not use consistent locking in some situations, leading to a read-after-free vulnerability. A local attacker could use this to cause a denial of service (system crash) or possibly expose sensitive information (kernel memory). De4dCr0w of 360 Alpha Lab discovered that the BPF verifier in the Linux kernel did not properly handle mod32 destination register truncation when the source register was known to be 0. A local attacker could use this to expose sensitive information (kernel memory) or possibly execute arbitrary code. Various other vulnerabilities were also addressed.

tags | advisory, denial of service, arbitrary, kernel, local, vulnerability
systems | linux
advisories | CVE-2020-29660, CVE-2020-29661, CVE-2021-3444, CVE-2021-3715
SHA-256 | 4c43b77dc14ec38d515895508c90603e29e4435a67390143e2cb91e68bc70e9d

Download | Favorite | View

Related Files

Share This

Like Twee LinkedIn Reddit Digg StumbleUpon

Change Mirror Download

```
Linux kernel vulnerabilities

A security issue affects these releases of Ubuntu and its derivatives:

-   Ubuntu 20.04 LTS
-   Ubuntu 18.04 LTS
-   Ubuntu 16.04 ESM

Summary

Several security issues were fixed in the kernel.

Software Description

-   linux - Linux kernel
-   linux-gcp - Linux kernel for Google Cloud Platform (GCP) systems
-   linux-gke - Linux kernel for Google Container Engine (GKE) systems
-   linux-gkeop - Linux kernel for Google Container Engine (GKE) systems
-   linux-oem - Linux kernel for OEM systems

Details

Jann Horn discovered that the tty subsystem of the Linux kernel did not
use consistent locking in some situations, leading to a read-after-free
vulnerability. A local attacker could use this to cause a denial of
service (system crash) or possibly expose sensitive information (kernel
memory). (CVE-2020-29660)

Jann Horn discovered a race condition in the tty subsystem of the Linux
kernel in the locking for the TIOCSPGRP ioctl(), leading to a use-after-
free vulnerability. A local attacker could use this to cause a denial of
service (system crash) or possibly execute arbitrary code.
(CVE-2020-29661)

De4dCr0w of 360 Alpha Lab discovered that the BPF verifier in the Linux
kernel did not properly handle mod32 destination register truncation
when the source register was known to be 0. A local attacker could use
this to expose sensitive information (kernel memory) or possibly execute
arbitrary code. (CVE-2021-3444)

kernel: use-after-free in route4_change() in net/sched/cls_route.c
(CVE-2021-3715)

Update instructions

The problem can be corrected by updating your kernel livepatch to the
following versions:

Ubuntu 20.04 LTS
    gcp - 82.2
    generic - 82.2
    gke - 82.2
    gkeop - 82.2
    lowlatency - 82.2

Ubuntu 18.04 LTS
    generic - 82.1
    generic - 82.2
    gke - 82.1
    gke - 82.2
    gkeop - 82.2
    lowlatency - 82.1
    lowlatency - 82.2
    oem - 82.1
    oem - 82.2

Ubuntu 16.04 ESM
    generic - 82.1
    generic - 82.2
    lowlatency - 82.1
    lowlatency - 82.2

Support Information

Kernels older than the levels listed below do not receive livepatch
updates. If you are running a kernel version earlier than the one listed
below, please upgrade your kernel as soon as possible.

Ubuntu 20.04 LTS
    linux-aws - 5.4.0-1009
    linux-azure - 5.4.0-1010
    linux-gcp - 5.4.0-1009
    linux-gke - 5.4.0-1033
    linux-gkeop - 5.4.0-1009
    linux-oem - 5.4.0-26
    linux - 5.4.0-26

Ubuntu 18.04 LTS
    linux-aws - 4.15.0-1054
    linux-azure-4.15 - 4.15.0-1115
    linux-gke-4.15 - 4.15.0-1076
    linux-gke-5.4 - 5.4.0-1009
    linux-gkeop-5.4 - 5.4.0-1007
    linux-hwe-5.4 - 5.4.0-26
    linux-oem - 4.15.0-1063
    linux - 4.15.0-69

Ubuntu 16.04 ESM
    linux-aws - 4.4.0-1098
    linux-azure - 4.15.0-1063
    linux-hwe - 4.15.0-69
    linux - 4.4.0-168

Ubuntu 14.04 ESM
    linux-lts-xenial - 4.4.0-168

References

-   CVE-2020-29660
-   CVE-2020-29661
-   CVE-2021-3444
-   CVE-2021-3715
```

Follow us on Twitter

Subscribe to an RSS Feed

File Archive: December 2022 <

Su	Mo	Tu	We	Th	Fr	Sa
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31

Top Authors In Last 30 Days

Red Hat	150 files
Ubuntu	68 files
LiquidWorm	23 files
Debian	16 files
malvuln	11 files
nu11secur1ty	11 files
Gentoo	9 files
Google Security Research	6 files
Julien Ahrens	4 files
T. Weber	4 files

File Tags

ActiveX	(932)
Advisory	(79,754)
Arbitrary	(15,694)
BBS	(2,859)
Bypass	(1,619)
CGI	(1,018)
Code Execution	(6,926)
Conference	(673)
Cracker	(840)
CSRF	(3,290)
DoS	(22,602)
Encryption	(2,349)
Exploit	(50,359)
File Inclusion	(4,165)
File Upload	(946)
Firewall	(821)
Info Disclosure	(2,660)
Intrusion Detection	(867)
Java	(2,899)
JavaScript	(821)
Kernel	(6,291)
Local	(14,201)
Magazine	(586)
Overflow	(12,419)
Perl	(1,418)
PHP	(5,093)
Proof of Concept	(2,291)
Protocol	(3,435)
Python	(1,467)
Remote	(30,044)
Root	(3,504)
Ruby	(594)
Scanner	(1,631)
Security Tool	(7,777)
Shell	(3,103)
Shellcode	(1,204)
Sniffer	(886)

File Archives

December 2022
November 2022
October 2022
September 2022
August 2022
July 2022
June 2022
May 2022
April 2022
March 2022
February 2022
January 2022
Older

Systems

AIX	(426)
Apple	(1,926)
BSD	(370)
CentOS	(55)
Cisco	(1,917)
Debian	(6,634)
Fedora	(1,690)
FreeBSD	(1,242)
Gentoo	(4,272)
HPUX	(878)
iOS	(330)
iPhone	(108)
IRIX	(220)
Juniper	(67)
Linux	(44,315)
Mac OS X	(684)
Mandriva	(3,105)
NetBSD	(255)
OpenBSD	(479)
RedHat	(12,469)
Slackware	(941)
Solaris	(1,607)

```
--
ubuntu-security-announce mailing list
ubuntu-security-announce@lists.ubuntu.com
Modify settings or unsubscribe at: https://lists.ubuntu.com/mailman/listinfo/ubuntu-security-announce
```

Login or Register to add favorites

Spoof (2,166)
SQL Injection (16,102)
TCP (2,379)
Trojan (686)
UDP (876)
Virus (662)
Vulnerability (31,136)
Web (9,365)
Whitepaper (3,729)
x86 (946)
XSS (17,494)
Other

SUSE (1,444)
Ubuntu (8,199)
UNIX (9,159)
UnixWare (185)
Windows (6,511)
Other

Site Links
News by Month
News Tags
Files by Month
File Tags
File Directory

About Us
History & Purpose
Contact Information
Terms of Service
Privacy Statement
Copyright Information

Hosting By
Rokasec

Follow us on Twitter

Subscribe to an RSS Feed