Register | Login

packet storm
what you don't know can hurt you

Search …

| Home | Files | News | About | Contact |&[SERVICES_TAB] | Add New |

Kernel Live Patch Security Notice LSN-0086-1

Authored by Benjamin M. Romer

Posted Jun 3, 2022

It was discovered that a race condition existed in the network scheduling subsystem of the Linux kernel, 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. Yiqi Sun and Kevin Wang discovered that the cgroups implementation in the Linux kernel did not properly restrict access to the cgroups v1 release_agent feature. A local attacker could use this to gain administrative privileges. Various other issues were also addressed.

tags | advisory, denial of service, arbitrary, kernel, local
systems | linux
advisories | CVE-2021-39713, CVE-2022-0492, CVE-2022-1055, CVE-2022-1116, CVE-2022-21499, CVE-2022-29581, CVE-2022-30594
SHA-256 | d764344ffd074691e5125e0c7ecb9972329d587b004cdad9acfe1fafabfb0253 **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
-   Ubuntu 22.04 LTS
-   Ubuntu 14.04 ESM

Summary

Several security issues were fixed in the kernel.

Software Description

-   linux - Linux kernel
-   linux-aws - Linux kernel for Amazon Web Services (AWS) systems
-   linux-azure - Linux kernel for Microsoft Azure Cloud systems
-   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-ibm - Linux kernel for IBM cloud systems
-   linux-oem - Linux kernel for OEM systems

Details

It was discovered that a race condition existed in the network
scheduling subsystem of the Linux kernel, 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-2021-39713)

Yiqi Sun and Kevin Wang discovered that the cgroups implementation in
the Linux kernel did not properly restrict access to the cgroups v1
release_agent feature. A local attacker could use this to gain
administrative privileges. (CVE-2022-0492)

It was discovered that the network traffic control implementation in the
Linux kernel contained 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-2022-1055)

Bing-Jhong Billy Jheng discovered that the io_uring subsystem in the
Linux kernel contained in integer overflow. A local attacker could use
this to cause a denial of service (system crash) or execute arbitrary
code. (CVE-2022-1116)

It was discovered that the Linux kernel did not properly restrict access
to the kernel debugger when booted in secure boot environments. A
privileged attacker could use this to bypass UEFI Secure Boot
restrictions. (CVE-2022-21499)

Kyle Zeng discovered that the Network Queuing and Scheduling subsystem
of the Linux kernel did not properly perform reference counting in some
situations, leading to a use-after-free vulnerability. A local attacker
could use this to cause a denial of service (system crash) or execute
arbitrary code. (CVE-2022-29581)

Jann Horn discovered that the Linux kernel did not properly enforce
seccomp restrictions in some situations. A local attacker could use this
to bypass intended seccomp sandbox restrictions. (CVE-2022-30594)

Update instructions

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

Ubuntu 20.04 LTS
    aws - 86.3
    azure - 86.3
    gcp - 86.3
    generic - 86.3
    gke - 86.3
    gkeop - 86.3
    ibm - 86.3
    lowlatency - 86.3

Ubuntu 18.04 LTS
    aws - 86.3
    azure - 86.3
    gcp - 86.3
    generic - 86.3
    gke - 86.3
    gkeop - 86.3
    ibm - 86.3
    lowlatency - 86.3
    oem - 86.3

Ubuntu 16.04 ESM
    aws - 86.3
    azure - 86.3
    gcp - 86.3
    generic - 86.3
    lowlatency - 86.3

Ubuntu 22.04 LTS
    gcp - 86.4
    generic - 86.4
    gke - 86.4
    ibm - 86.4
    lowlatency - 86.4

Ubuntu 14.04 ESM
    generic - 86.3
    lowlatency - 86.3

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-aws - 5.4.0-1061
```

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 157 files
Ubuntu 76 files
LiquidWorm 23 files
Debian 21 files
nu11secur1ty 11 files
malvuln 11 files
Gentoo 9 files
Google Security Research 8 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)

```
    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-hwe - 5.15.0-0
    linux-ibm - 5.4.0-1009
    linux-oem - 5.4.0-26
    linux - 5.4.0-26

Ubuntu 18.04 LTS
    linux-aws-5.4 - 5.4.0-1069
    linux-aws - 4.15.0-1054
    linux-azure-4.15 - 4.15.0-1115
    linux-azure-5.4 - 5.4.0-1069
    linux-gcp-4.15 - 4.15.0-1121
    linux-gcp-5.4 - 5.4.0-1069
    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-ibm-5.4 - 5.4.0-1009
    linux-oem - 4.15.0-1063
    linux - 4.15.0-69

Ubuntu 16.04 ESM
    linux-aws-hwe - 4.15.0-1126
    linux-aws - 4.4.0-1098
    linux-aws - 4.4.0-1129
    linux-azure - 4.15.0-1063
    linux-azure - 4.15.0-1078
    linux-azure - 4.15.0-1114
    linux-gcp - 4.15.0-1118
    linux-hwe - 4.15.0-143
    linux-hwe - 4.15.0-69
    linux - 4.4.0-168
    linux - 4.4.0-211

Ubuntu 22.04 LTS
    linux-aws - 5.15.0-1000
    linux-azure - 5.15.0-1000
    linux-gcp - 5.15.0-1000
    linux-gke - 5.15.0-1000
    linux-ibm - 5.15.0-1000
    linux - 5.15.0-24
    linux - 5.15.0-25

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

References

-   CVE-2021-39713
-   CVE-2022-0492
-   CVE-2022-1055
-   CVE-2022-1116
-   CVE-2022-21499
-   CVE-2022-29581
-   CVE-2022-30594
```

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

Login or Register to add favorites

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