Kernel Live Patch Security Notice LSN-0083-1

Authored by Benjamin M. Romer

Posted Jan 6, 2022

The BPF subsystem in the Linux kernel before 4.17 mishandles situations with a long jump over an instruction sequence where inner instructions require substantial expansions into multiple BPF instructions, leading to an overflow. This affects kernel/bpf/core.c and net/core/filter.c. Maxim Levitsky discovered that the KVM hypervisor implementation for AMD processors in the Linux kernel did not properly prevent a guest VM from enabling AVIC in nested guest VMs. An attacker in a guest VM could use this to write to portions of the host's physical memory. Other vulnerabilities have also been addressed.

tags | advisory, overflow, kernel, vulnerability
systems | linux
advisories | CVE-2018-25020, CVE-2021-22555, CVE-2021-33909, CVE-2021-3653, CVE-2021-4002
SHA-256 | ddd1e7fc677c2b02d3351058bf31466aa231865f93abfb9cdfa1d1ca55622f8d Download | Favorite | View

Related Files

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-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-oem - Linux kernel for OEM systems

Details

The BPF subsystem in the Linux kernel before 4.17
mishandles situations with a long jump over an instruction sequence
where inner instructions require substantial expansions into multiple
BPF instructions, leading to an overflow. This affects kernel/bpf/core.c
and net/core/filter.c. (CVE-2018-25020)

Maxim Levitsky discovered that the KVM hypervisor implementation for AMD
processors in the Linux kernel did not properly prevent a guest VM from
enabling AVIC in nested guest VMs. An attacker in a guest VM could use
this to write to portions of the host's physical memory. (CVE-2021-3653)

Nadav Amit discovered that the hugetlb implementation in the Linux
kernel did not perform TLB flushes under certain conditions. A local
attacker could use this to leak or alter data from other processes that
use huge pages. (CVE-2021-4002)

Andy Nguyen discovered that the netfilter subsystem in the Linux kernel
contained an out-of-bounds write in its setsockopt() implementation. A
local attacker could use this to cause a denial of service (system
crash) or possibly execute arbitrary code. (CVE-2021-22555)

It was discovered that the virtual file system implementation in the
Linux kernel contained an unsigned to signed integer conversion error. A
local attacker could use this to cause a denial of service (system
crash) or execute arbitrary code. (CVE-2021-33909)

Update instructions

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

Ubuntu 20.04 LTS
    aws - 83.1
    azure - 83.1
    gcp - 83.1
    generic - 83.1
    gke - 83.1
    gkeop - 83.1
    lowlatency - 83.1

Ubuntu 18.04 LTS
    aws - 83.1
    generic - 83.1
    gke - 83.1
    gke - 83.2
    gkeop - 83.1
    gkeop - 83.2
    lowlatency - 83.1
    oem - 83.1

Ubuntu 16.04 ESM
    aws - 83.1
    azure - 83.1
    generic - 83.1
    lowlatency - 83.1

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 - 4.15.0-143
    linux - 4.4.0-168

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


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)

```
References

-   CVE-2018-25020
-   CVE-2021-3653
-   CVE-2021-4002
-   CVE-2021-22555
-   CVE-2021-33909


--
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
```


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