USN-4886-1: Privoxy vulnerabilities

It was discovered that Privoxy incorrectly handled CGI requests. An attacker
could possibly use this issue to cause a denial of service or obtain sensitive
information. (CVE-2020-35502, CVE-2021-20209, CVE-2021-20210,
CVE-2021-20213, CVE-2021-20215, CVE-2021-20216, CVE-2021-20217,
CVE-2021-20272, CVE-2021-20273, CVE-2021-20275)
It was discovered that Privoxy incorrectly handled certain regular
expressions. An attacker could possibly use this issue to cause a denial of
service or obtain sensitive information. (CVE-2021-20212, CVE-2021-20276)

It was discovered that Privoxy incorrectly handled client tags. An attacker
could possibly use this issue to cause Privoxy to consume resources, resulting
in a denial of service. This issue only affected Ubuntu 18.04 LTS,
Ubuntu 20.04 LTS and Ubuntu 20.10. (CVE-2021-20211)

It was discovered that Privoxy incorrectly handled client tags. An attacker
could possibly use this issue to cause Privoxy to consume resources, resulting
in a denial of service. This issue only affected Ubuntu 20.04 LTS and
Ubuntu 20.10. (CVE-2021-20214)

USN-4885-1: Pygments vulnerability

It was discovered that Pygments incorrectly handled parsing SML files. If a
user or automated system were tricked into parsing a specially crafted SML
file, a remote attacker could cause Pygments to hang, resulting in a denial
of service.

USN-4884-1: Linux kernel (OEM) vulnerabilities

Loris Reiff discovered that the BPF implementation in the Linux kernel did
not properly validate attributes in the getsockopt BPF hook. A local
attacker could possibly use this to cause a denial of service (system
crash). (CVE-2021-20194)
It was discovered that the priority inheritance futex implementation in the
Linux kernel contained a race condition, 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-2021-3347)

It was discovered that the network block device (nbd) driver in the Linux
kernel contained a use-after-free vulnerability during device

setup. A
local attacker with access to the nbd device could use this to cause a
denial of service (system crash) or possibly execute arbitrary code.
(CVE-2021-3348)

USN-4883-1: Linux kernel vulnerabilities

Adam Nichols discovered that heap overflows existed in the iSCSI subsystem
in the Linux kernel. A local attacker could use this to cause a denial of
service (system crash) or possibly execute arbitrary code. (CVE-2021-27365)
Adam Nichols discovered that the iSCSI subsystem in the Linux kernel did
not properly restrict access to iSCSI transport handles. A local attacker
could use this to cause a denial of service or expose sensitive information
(kernel pointer addresses). (CVE-2021-27363)

Adam Nichols discovered that an out-of-bounds read existed in the iSCSI
subsystem in the Linux kernel. A local attacker could use this to cause a
denial of service (system crash) or expose sensitive information (kernel
memory). (CVE-2021-27364)

[CentOS-announce] CESA-2021:0856 Important CentOS 7 kernel Security Update

CentOS Errata and Security Advisory 2021:0856 Important
Upstream details at : https://access.redhat.com/errata/RHSA-2021:0856

The following updated files have been uploaded and are currently

syncing to the mirrors: (sha256sum Filename)

x86_64:

a6119606e76fc09a37585914c2063026064b1b979d9cffcf71712c2218b4c3c2 bpftool-3.10.0-1160.21.1.el7.x86_64.rpm

b8c980b0d2eaf56affe69fde8c004c91dde7d83277578de4cfc8c06aaa322858 kernel-3.10.0-1160.21.1.el7.x86_64.rpm

62db43a91b2c1f3cd0407729f5c13f51ea098fea0aa9b90e2444d92166d1817d kernel-abi-whitelists-3.10.0-1160.21.1.el7.noarch.rpm

b918eb715248bdb46d8f49387310a25030a9f4fe192d5ee0f69fabde9b84d42d kernel-debug-3.10.0-1160.21.1.el7.x86_64.rpm

3f77e8c91079e010fb161e28eaf613452e1c25d2d67b0367cb344f3141bf3cb9 kernel-debug-devel-3.10.0-1160.21.1.el7.x86_64.rpm

4abf0ebc2127e7a5b5dfb595fa447cb44f339ff023ce88bb0a97992bba4cd3a9 kernel-devel-3.10.0-1160.21.1.el7.x86_64.rpm

29feb5e5f9922979d66fabe2aac8bd7fdd18f1915777acf5b360bb7e5cdb0109 kernel-doc-3.10.0-1160.21.1.el7.noarch.rpm

21af3e26269599f29ef700b687a3e84539aa03ffc025f0794649d54f0a041582 kernel-headers-3.10.0-1160.21.1.el7.x86_64.rpm

a133fe2fda391e345abde6444e57c6fbfb5ebcfe7720bc5b1ae1c3313bd38aed kernel-tools-3.10.0-1160.21.1.el7.x86_64.rpm

34255ef50bd9c16239a9a579c23a1bc1f046428a2aecf0fb06e04340b46af985 kernel-tools-libs-3.10.0-1160.21.1.el7.x86_64.rpm

6a47e214a36fc58ad9b00ab50073240c79076c8bd04a01dd01029f8ca43122bd kernel-tools-libs-devel-3.10.0-1160.21.1.el7.x86_64.rpm

2520a8d9459f82ba9401fb0a86ddb5154277672b55919b252535b199ef9fc3d4 perf-3.10.0-1160.21.1.el7.x86_64.rpm

9308a731a1aba4b9209f5cc4ee3e7f8bd57be5fa213ed219fd59941fb9b092cb python-perf-3.10.0-1160.21.1.el7.x86_64.rpm

Source:

26eccba611785427726d6ecdb0a26f910a6ac05b29f3f6e3afd12f4d363a52f9 kernel-3.10.0-1160.21.1.el7.src.rpm

_

Johnny Hughes

CentOS Project { http://www.centos.org/ }

irc: hughesjr, #[hidden email]

Twitter: @JohnnyCentOS

_____

CentOS-announce mailing list

[hidden email]

https://lists.centos.org/mailman/listinfo/centos-announce