Security Leftovers

By *Roy Schestowitz*
Created *21/07/2021 - 3:24pm*
Submitted by Roy Schestowitz on Wednesday 21st of July 2021 03:24:07 PM Filed under Security [1]

- **Authorization Basics [2]**

  In this article, we explained what authorization is and how it differs from authentication. We gave examples for authorization processes and explained the two different access control models: capability-based access control and access control lists.

  The Linux/UNIX file permissions were used to show an example of how ACLs could be used. Note that, although Linux/UNIX file permissions are a type of ACL, they are not to be confused with the POSIX ACL, which are also available on Linux platforms. S acl(5) in the man pages for more information.

  We learned that authorization is used to determine what actions a subject is allowed to perform on an object. Besides the examples from this article, other methods can be used to implement access control, including Discretionary Access Control (DAC), Mandatory Access Control (MAC) or Role-Based Access Control (RBAC), to name the most common ones.

- **Security updates for Wednesday [3]**

  Security updates have been issued by Arch Linux (ant, code, dino, firefox-ublock-origin, go, libuv, nextcloud-app-mail, nodejs-lts-erbium, nodejs-lts-fermium, openvswitch, putty, racket, telegram-desktop, and wireshark-cli), Debian (kernel, linux-4.19, and systemd), Fedora (kernel, kernel-headers, kernel-tools, and krb5), Gentoo (systemd), Mageia (perl-Convert-ASN1 and wireshark), openSUSE (caribou, containerd, crmsh, fossil, icinga2, kernel, nextcloud, and systemd), Red Hat (389-ds:1.4, glibc, java-1.8.0-openjdk, java-11-openjdk, kernel, kernel-rt, kpatch-patch, libldb, perl, RHV-H, rpm, shim and fwupd, and systemd), Slackware (kernel), SUSE (caribou, containerd, crmsh, curl, dbus-1, kernel, qemu, and

systemd), and Ubuntu (binutils, linux, linux-aws, linux-aws-5.4, linux-azure, linux-azure-5.4, linux-gcp, linux-gcp-5.4, linux-gke, linux-gke-5.4, linux-gkeop, linux-gkeop-5.4, linux-hwe-5.4, linux-kvm, linux-oracle, linux-oracle-5.4, linux-raspi, linux-raspi-5.4, linux, linux-aws, linux-aws-5.8, linux-azure, linux-azure-5.8, linux-gcp, linux-gcp-5.8, linux-hwe-5.8, linux-kvm, linux-oracle, linux-oracle-5.8, linux-raspi, linux, linux-aws, linux-aws-hwe, linux-azure, linux-azure-4.15, linux-gcp, linux-gcp-4.15, linux-hwe, linux-kvm, linux-oracle, linux-raspi2, linux-snapdragon, linux, linux-aws, linux-azure, linux-gcp, linux-gke-5.3, linux-hwe, linux-lts-xenial, linux-kvm, linux-oracle, linux-raspi, linux-raspi2-5.3, linux-oem-5.10, nvidia-graphics-drivers-390, nvidia-graphics-drivers-418-server, nvidia-graphics-drivers-450-server, nvidia-graphics-drivers-460, nvidia-graphics-drivers-460-server, nvidia-graphics-drivers-470, and systemd).

- **NVIDIA announce new security issues, make sure you have updated drivers [4]**

  Here we are again. NVIDIA has today sent out a security bulletin to inform users on Linux and Windows to ensure your GPU drivers are up to date to do freshly revealed security problems.

  The issues can result in information disclosure, data tampering, and denial of service. As always, even if you think you're not vulnerable for whatever reason, upgrading is highly recommended now.

- **Defending Against Spyware Like Pegasus [5]**

  This has been a busy week for security news, but perhaps the most significant security and privacy story to break this week (if not this year), is about how NSO Group?s Pegasus spyware has been used by a number of governments to infect and spy on journalists and activists and even heads of state by sending an invisible, silent attack to their iPhone that requires no user interaction. This attack works even on new, fully-patched phones, and once the phone is compromised, the attacker has full remote control over the phone including access to the file system, location, and microphone and cameras.

  What?s particularly scary about spyware in general, and is true for Pegasus as well, is that victims have no indication they?ve been compromised. Due to how locked down the iPhone is from the end user, detecting Pegasus in particular requires expert forensics techniques. This has left many at-risk iPhone users wondering whether they too are compromised and if so, what do they do?

Security

Source URL: http://www.tuxmachines.org/node/153648

Links:

[1] http://www.tuxmachines.org/taxonomy/term/59
[2] https://www.fosslife.org/authorization-basics
[3] https://lwn.net/Articles/863861/rss
[4] https://www.gamingonlinux.com/2021/07/nvidia-announce-new-security-issues-make-sure-you-have-updated-drivers
[5] https://puri.sm/posts/defending-against-spyware-like-pegasus/