Security Leftovers

By *Roy Schestowitz*
Created *29/07/2021 - 2:31am*
Submitted by Roy Schestowitz on Thursday 29th of July 2021 02:31:24 AM Filed under Security [1]

- **[JumpCloud] Recent Linux Releases: Desktop MFA & Security Commands [2]**

  Operating system diversity is a defining characteristic of today?s IT environments. Windows may have dominated historically, but enterprise Mac management has evolved in a meaningful way and Linux distributions have become a critical part of IT infrastructure. Cross-OS device management is here to stay, and presents a unique challenge for IT admins.

  Linux in particular can be a complex beast to manage because unlike MacOS and Windows, it is not a proprietary OS and can be found across multiple distros. There are many benefits to this openness however, including cost, interoperability, and flexibility. These factors, and more, have led to a strong Linux following among its community of users.

  With an increasing number of employee workstations running a wide variety of Linux distros, administrators need a way to increase visibility into their fleets, and improve the management of not only Linux systems, but Mac and Windows as well. IT admins can use the JumpCloud Directory Platform to comprehensively accomplish these tasks, thanks to the recent Linux releases detailed in this article.

- **Mozilla Security Blog: Making Client Certificates Available By Default in Firefox 90 [3]**

  Starting with version 90, Firefox will automatically find and offer to use client authentication certificates provided by the operating system on macOS and Windows. This security and usability improvement has been available in Firefox since version 75, but previously end users had to manually enable it.

  When a web browser negotiates a secure connection with a website, the web server sends a

certificate to the browser to prove its identity. Some websites (most commonly corporate authentication systems) request that the browser sends a certificate back to it as well, so that the website visitor can prove their identity to the website (similar to logging in with a username and password). This is sometimes called ?mutual authentication?.

- **The Sequoia seq_file vulnerability [4]**

  A local root hole in the Linux kernel, called Sequoia, was disclosed by Qualys on July 20. A full system compromise is possible until the kernel is patched (or mitigations that may not be fully effective are applied). At its core, the vulnerability relies on a path through the kernel where 64-bit size_t values are "converted" to signed integers, which effectively results in an overflow. The flaw was reported to Red Hat on June 9, along with a local systemd denial-of-service vulnerability, leading to a kernel crash, found at the same time. Systems with untrusted local users need updates for both problems applied as soon as they are available?out of an abundance of caution, other systems likely should be updated as well.

  Down in the guts of the kernel's seq_file interface, which is used for handling virtual files in /proc and the like, buffers are needed to store each line of the file's "contents". To start, a page of memory is allocated for the buffer, but if that is not sufficient, a new buffer that is twice the size of the old one is allocated. This is all done using a size_t, which is an unsigned 64-bit quantity (on x86_64) that is large enough to hold the results, so "the system would run out of memory long before this multiplication overflows".

Security

Links:
[1] http://www.tuxmachines.org/taxonomy/term/59
[2] https://jumpcloud.com/blog/linux-releases-desktop-mfa-security-commands
[3] https://blog.mozilla.org/security/2021/07/28/making-client-certificates-available-by-default-in-firefox-90/
[4] https://lwn.net/Articles/863729/