USN-4717-2: Firefox regression

USN-4717-1 fixed vulnerabilities in Firefox. The update caused a startup hang in some circumstances. This update fixes the problem.
We apologize for the inconvenience.

Original advisory details:

Multiple security issues were discovered in Firefox. If a user were tricked in to opening a specially crafted website, an attacker could potentially exploit these to cause a denial of service, obtain sensitive information, conduct clickjacking attacks, or execute arbitrary code.

USN-4713-2: Linux kernel vulnerability

It was discovered that the LIO SCSI target implementation in the Linux kernel performed insufficient identifier checking in certain XCOPY requests. An attacker with access to at least one LUN in a multiple backstore environment could use this to expose sensitive information or modify data.

USN-4728-1: snapd vulnerability

Gilad Reti discovered that snapd did not correctly specify cgroup
delegation when generating systemd service units for various container
management snaps. This could allow a local attacker to escalate privileges
via access to arbitrary devices of the container host from within a
compromised or malicious container.

USN-4727-1: Linux kernel vulnerability

Alexander Popov discovered that multiple race conditions existed in the
AF_VSOCK implementation in the Linux kernel. A local attacker could use
this to cause a denial of service (system crash) or execute arbitrary code.

USN-4726-1: OpenJDK

vulnerability

It was discovered that OpenJDK incorrectly handled the direct buffering of characters. An attacker could use this issue to cause OpenJDK to crash, resulting in a denial of service, or cause other unspecified impact.