

USN-4761-1: Git vulnerability

Matheus Tavares discovered that Git incorrectly handled delay-capable clean/smudge filters when being used on case-insensitive filesystems. A remote attacker could possibly use this issue to execute arbitrary code.

USN-4758-1: Go vulnerability

It was discovered that Go applications incorrectly handled uploaded content. If a user were tricked into visiting a malicious page, a remote attacker could exploit this with a crafted file to conduct cross-site scripting (XSS) attacks.

USN-4760-1: libzstd vulnerabilities

It was discovered that libzstd incorrectly handled file permissions. A local attacker could possibly use this issue to access certain files, contrary to expectations.

USN-4759-1: vulnerabilities

GLib

Krzyszimir Nowak discovered that GLib incorrectly handled certain large buffers. A remote attacker could use this issue to cause applications linked to GLib to crash, resulting in a denial of service, or possibly execute arbitrary code. (CVE-2021-27218)

Kevin Backhouse discovered that GLib incorrectly handled certain memory allocations. A remote attacker could use this issue to cause applications linked to GLib to crash, resulting in a denial of service, or possibly execute arbitrary code. (CVE-2021-27219)

USN-4733-2: GNOME Autoar regression

USN-4733-1 fixed a vulnerability in GNOME Autoar. The upstream fix introduced a regression when extracting archives containing directories. This update fixes the problem. Original advisory details:

Yiğit Can Yılmaz discovered that GNOME Autoar could extract files outside of the intended directory. If a user were tricked into extracting a

specially crafted archive, a remote attacker could create files in arbitrary locations, possibly leading to code execution.