USN-4893-1: Firefox vulnerabilities

Multiple security issues were discovered in Firefox. If a user were
tricked into opening a specially crafted website, an attacker could
potentially exploit these to cause a denial of service, obtain sensitive
information, or execute arbitrary code. (CVE-2021-23981, CVE-2021-23982,
CVE-2021-23983, CVE-2021-23987, CVE-2021-23988)
It was discovered that extensions could open popup windows with control
of the window title in some circumstances. If a user were tricked into
installing a specially crafted extension, an attacker could potentially
exploit this to spook a website and trick the user into providing
credentials. (CVE-2021-23984)

It was discovered that the DevTools remote debugging feature could be
enabled without an indication to the user. If a local attacker could
modify the browser configuration, a remote attacker could potentially
exploit this to obtain sensitive information. (CVE-2021-23985)

It was discovered that extensions could read the response of cross
origin requests in some circumstances. If a user were tricked into
installing a specially crafted extension, an attacker could potentially
exploit this to obtain sensitive information. (CVE-2021-23986)